AD-A284 588

Defense Nuclear Agency
Alexandria, VA 22310-3398

DNA-TR-94-6

Biometric Identification Verification Technology Status and Feasibility Study

John E. Siedlarz, et al.
IraScan Incorporated
133-Q Gaither Drive
Mt. Laurel, NJ 08054

September 1994

Technical Report

CONTRACT No. DNA 001-93-C-0137

Approved for public release;
distribution is unlimited.

DISTRIBUTION LIST UPDATE

This mailer is provided to enable DNA to maintain current distribution lists for reports. (We would appreciate your providing the requested information.)

- ☐ Add the individual listed to your distribution list.
- ☐ Delete the cited organization/individual.
- ☐ Change of address.

NOTE:
Please return the mailing label from the document so that any additions, changes, corrections or deletions can be made easily. For distribution cancellation or more information call DNA/IMAS (703) 325-1036.

NAME: ______________________________

ORGANIZATION: ______________________________

OLD ADDRESS	**CURRENT ADDRESS**

TELEPHONE NUMBER: ( ) ______________________________

DNA PUBLICATION NUMBER/TITLE	**CHANGES/DELETIONS/ADDITIONS, etc.)** *(Attach Sheet if more Space is Required)*

DNA OR OTHER GOVERNMENT CONTRACT NUMBER: ______________________________

CERTIFICATION OF NEED-TO-KNOW BY GOVERNMENT SPONSOR (if other than DNA):

SPONSORING ORGANIZATION: ______________________________

CONTRACTING OFFICER OR REPRESENTATIVE: ______________________________

SIGNATURE: ______________________________

CUT HERE AND RETURN

DEFENSE NUCLEAR AGENCY
ATTN: IMAS
6801 TELEGRAPH ROAD
ALEXANDRIA, VA 22310-3398

DEFENSE NUCLEAR AGENCY
ATTN: IMAS
6801 TELEGRAPH ROAD
ALEXANDRIA, VA 22310-3398

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE: 940901

3. REPORT TYPE AND DATES COVERED: Technical 930719 – 931217

4. TITLE AND SUBTITLE

Biometric Identification Verification Technology Status and Feasibility Study

5. FUNDING NUMBERS

C - DNA 001-93-C-0137
PE -
PR - RF
TA - DA
WU - DH 348500

6. AUTHOR(S)

John E. Siedlarz, Cletus B. Kuhla, Gerald O. Williams, James T. McHugh, and Donald R. Richards

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IraScan Incorporated
133-Q Gaither Drive
Mt. Laurel, NJ 08054

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Nuclear Agency
6801 Telegraph Road
Alexandria, VA 22310-3398
NOSA/Gore

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

DNA-TR-94-6

11. SUPPLEMENTARY NOTES

This work was sponsored by the Defense Nuclear Agency under RDT&E RMC Code B2638D RF DA 00014 2520A AE 25904D.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

DoD cost and personnel reductions drive requirements for an entry/access control system capable of identifying and verifying the identity of persons with a high degree of confidence and without a man in the decision loop. Operational Performance Requirements (OPR) were assembled from the SOW and Service requirements documents. An extensive search for biometric information in the DTIC and NTIS databases was conducted. The capabilities of biometric identification systems available on the market and in known R&D programs were verified wherever possible by independent tests and evaluations. Technologies included were fingerprint, palmprint, hand geometry, signature, voice, retina scan, facial recognition and iris scan.
The study found no system, technology or methodology which can currently meet all of the objectives and requirements specified in the SOW. Of all the technologies/systems under development, only the IriScan process appears capable, with further development, of meeting the desired objectives and OPRs.

14. SUBJECT TERMS

Biometric | Recognition
Access Control | Identification

15. NUMBER OF PAGES: 118

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAR

CLASSIFIED BY:

N/A since Unclassified.

DECLASSIFY ON:

N/A since Unclassified.

Accesion For	
NTIS CRA&I	☑
DTIC TAB	☐
Unannounced	☐
Justification	
By	
Distribution /	
Availability Codes	
Dist	Avail and / or Special
A-1	

EXECUTIVE SUMMARY

There is a need within the Department of Defense (DoD) to provide an entry/access control system capable of identifying and verifying the identity of persons with a high degree of confidence and without a man in the loop. In support of this requirement, the Defense Nuclear Agency (DNA) reached a preliminary conclusion as to the most promising technology to pursue, and initiated this study effort to confirm or refute their conclusion, and to determine the feasibility of developing the selected system. This study looked at all systems available on the market and compared their effectiveness against the Operational Performance Requirements (OPR) specified. R & D systems and technologies which appear to have the potential to meet the specifications were also reviewed. Primarily, these were voice, facial and iris recognition.

The study found no system, technology, or methodology which can currently meet all of the objectives and requirements specified in the Statement of Work (SOW). Further, of the systems, technologies, and methodologies under development, only the IriScan system of positive identification verification, using an iris recognition process, appears capable, with further development, of meeting those objectives and OPRs. Based on our research, the primary alternatives of voice and facial recognition cannot now, or in the foreseeable future, meet many of the stringent requirements for DoD application. Their inherent inability to satisfy critical criteria cannot be overcome in the near future by additional cost effective development.

The study also contains additional information to sustain a development decision by defining Support System Requirements, Technical System Requirements, and Operational Scenarios, and providing a System Design Concept and a Strawman Deployment POA&M. Finally, rough order of magnitude cost estimates to complete development, to provide a core system and to install a portal are provided.

CONVERSION TABLE

Conversion factors for U.S. customary to metric (SI) units of measurement

To Convert From	To	Multiply
angstrom	meters (m)	1.000 000 X E-10
atmosphere (normal)	kilo pascal (kPa)	1.013 25 X E+2
bar	kilo pascal (kPa)	1.000 000 X E+2
barn	meter^2 (m^2)	1.000 000 X E-28
British Thermal unit (thermochemical)	joule (J)	1.054 350 X E+3
calorie (thermochemical)	joule (J)	4.184 000
cal (thermochemical)/cm^2	mega joule/m^2(MJ/m^2)	4.184 000 X E-2
curie	giga becquerel (GBq)*	3.700 000 X E+1
degree (angle)	radian (rad)	1.745 329 X E-2
degree Fahrenheit	degree kelvin (K)	$t_K=(t°F + 459.67)/1.8$
electron volt	joule (J)	1.602 19 X E-19
erg	joule (J)	1.000 000 X E-7
erg/second	watt (W)	1.000 000 X E-7
foot	meter (m)	3.048 000 X E-1
foot-pound-force	joule (J)	1.355 818
gallon (U.S. liquid)	meter^3 (m^3)	3.785 412 X E-3
inch	meter (m)	2.540 000 X E-2
jerk	joule (J)	1.000 000 X E+9
joule/kilogram (J/Kg) (radiation dose absorbed)	Gray (Gy)	1.000 000
kilotons	terajoules	4.183
kip (1000 lbf)	newton (N)	4.448 222 X E+3
kip/inch^2 (ksi)	kilo pascal (kPa)	6.894 757 X E+3
ktap	newton-second/m^2 (N-s/m^2)	1.000 000 X E+2
micron	meter (m)	1.000 000 X E-6
mil	meter (m)	2.540 000 X E-5
mile (international)	meter (m)	1.609 344 X E+3
ounce	kilogram (kg)	2.834 952 X E-2
pound-force (lbf avoirdupois)	newton (N)	4.448 222
pound-force inch	newton-meter (N·m)	1.129 848 X E-1
pound-force/inch	newton/meter (N/m)	1.751 268 X E+2
pound-force/foot^2	kilo pascal (kPa)	4.788 026 X E-2
pound-force/inch^2 (psi)	kilo pascal (kPa)	6.894 757
pound-mass (lbm avoirdupois)	kilogram (kg)	4.535 924 X E-1
pound-mass-foot^2 (moment of inertia)	kilogram-meter^2 (kg·m^2)	4.214 011 X E-2
pound-mass/foot^3	kilogram/meter^3 (kg/m^3)	1.601 846 X E+1
rad (radiation dose absorbed)	Gray (Gy)**	1.000 000 X E-2
roentgen	coulomb/kilogram (C/kg)	2.579 760 X E-4
shake	second (s)	1.000 000 X E-8
slug	kilogram (kg)	1.459 390 X E+1
torr (mm Hg, 0°C)	kilo pascal (kPa)	1.333 22 X E-1

*The becquerel (Bq) is the SI unit of radioactivity; Bp = 1 event/s.

**The Gray (Gy) is the SI unit of absorbed radiation.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

SECTION 1

INTRODUCTION

1.1 GENERAL.

Protection of assets, information, and people is normally accomplished by keeping the "bad guys" away and allowing access only to the "good guys". This has historically been accomplished by pre-identifying those who must have access (or entry), and treating everyone else as "bad guys." The issue is then reduced to one of positive identification and control. Traditionally, this has been accomplished by posting a guard or entry controller capable of visually recognizing each of the "good guys" or the identification media they carry. The computer age opened the possibility of automated personal identification, with higher accuracy and lower cost.

1.2 BACKGROUND.

Currently available personnel identification verification and entry control systems, biometric and non-biometric, have not yet been able to meet all operational requirements. They are generally manpower intensive, costly to procure and maintain, frequently unreliable, and sometimes slow in identifying individuals and verifying approved access. However, significant research and development in the field of biometric identification continues.

Experimental biometric personal identification systems have been built based on an extensive list of technologies, to include; fingerprints, thumb prints, palm prints, full-finger prints, hand shape, hand topography, hand geometry, signature verification, signature dynamics, keystroke dynamics, typing rhythms, wrist veins, hand veins, voice patterns, voice prints, lip prints, blood-vessel patterns in the retina of the eye, facial recognition, facial thermography, and feature patterns in the iris of the eye. More than 75 companies/organizations have performed research and development in one or more of these technologies. Many have experienced great difficulty in economically meeting high system accuracy and reliability requirements in rigorous field use. Many R&D projects have been initiated, but only a small percentage result in products reaching the market.

Systems which have reached the marketplace include fingerprint, thumbprint, hand geometry, keystroke dynamics, signature dynamics, voice patterns, retina patterns, and facial recognition. However, user dissatisfaction due to the operating problems identified above, as well as to the intrusiveness of some systems, has limited the number of available biometric identification products to about half a dozen at any one time.

The U. S. Air Force is the Department of Defense (DoD) Executive Agent for entry (access) control. Air Force entry control requirements are designated in Air Force Operational Requirements Document (ORD) 004-88. These requirements are further defined in the Advanced Entry Control System (AECS) Specification, including joint service criteria. In support of these requirements, the Defense Nuclear Agency (DNA) issued a Request for Proposal (RFP) seeking technologies meeting the requirements of that program. Iris identification technology was chosen based on the proposals submitted. This study was initiated to confirm the selection and determine the feasibility of developing an identification verification (IV) system capable of positively identifying and verifying individuals without physical contact and without a person in the decision loop. If a viable technology with high development potential can be identified, further research and development may be funded in order to provide a valid proof-of-concept prototype.

1.3 METHODOLOGY.

This Identification Verification (IV) Technology/Methodology Study was undertaken by IriScan, Inc., to investigate all previous and on-going IV research and development, and determine, to the maximum extent possible, the potential of meeting the defined operational requirements. The following methodology was utilized in conducting the study:

a. Delineate established operational and technical requirements for the IV system.

b. Research accessible government data repositories for IV system and R&D project information. Obtain copies of pertinent reports.

c. Collect IV system and R&D project information from professional, industrial, and other governmental sources.

d. Develop a Performance, Operational & Technical Requirements Matrix and complete it with system/R&D project data obtained.

e. Identify critical system criteria (requirements) and eliminate the systems/projects which do not meet these criteria.

f. Research and analyze candidate technologies, systems and projects for operational and technical capability to meet stated requirements.

g. Identify the specific technology/system/project which has the highest long-term potential to meet all requirements.

h. Articulate a Design Concept for the candidate system. Estimate costs to complete system development, produce system units, and install each system.

SECTION 2

SYSTEM REQUIREMENTS

2.1 SOURCES OF REQUIREMENTS.

Technical, operational, and performance requirements for the identification verification (IV) system came from several sources. Primarily, system requirements were obtained from the Statement of Work (SOW) included in DNA Contract DNA001-93-C-0137, with additional information from U. S. Air Force ORD 004-88 and the AECS Specification. Other data elements considered important to system development decision-making were derived from these sources. These requirements and data elements are included in the Performance, Operational, and Technical Requirements Matrix (Appendix A).

2.2 PERFORMANCE, OPERATIONAL AND TECHNICAL REQUIREMENTS.

2.2.1 Performs Verification.

The system must be capable of verifying that the biometric data captured from an entrant matches the biometric file in the database associated with the entrant's card, Personal Identification Number (PIN), or other pre-selected data file information.

2.2.2 Performs Identification.

The system must be capable of identifying an entrant based upon captured biometric data alone, without the use of card, PIN, or other data for establishing the identity of the entrant.

2.2.3 No Man In the Loop.

System operation is automatic. The entrance authorization or rejection decision occurs based upon comparison of captured biometric data with a database file, without human intervention or judgment.

2.2.4 No Contact.

The system functions, from biometric data capture through the entrance authorization or rejection decision, without physical contact between the entrant and the system.

2.2.5 Non-Invasive.

The capture of biometric data is not an invasive procedure. The system does not utilize images, tissues, or fluids from inside the human body, nor imprints of the exterior of the body.

2.2.6 Type I False Reject Error Rate.

The system falsely rejects less than one authorized entrant in 100 authorized entrance attempts (<1.0%).

2.2.7 Type II False Accept Error Rate.

The system falsely accepts less than one imposter in 1,000 imposter entrance attempts (<0.1%).

2.2.8 Crossover Error Rate. (Derived Requirement)

Many biometric IV systems have sensitivity adjustments. These systems can be set to minimize false accept errors, or at the other end of the scale, to reduce false reject errors. When a system is set to minimize false accept errors, false reject errors usually increase significantly. When set to reduce false reject errors, false accept errors increase. For example, a system set to achieve 0.1% false accepts, may have a false reject rate of 8%. When set to achieve a 1% false reject rate, the false accept rate may be 2%. This system could be said to meet both error standards; however, it could not meet them both simultaneously.

A single, better standard of system accuracy is the Crossover Error Rate. This is the measure of accuracy when the system is adjusted so that the false accept and false reject errors are equal. This setting is the one most likely to be utilized for normal system operations. A Crossover Rate less than 0.1% achieves both Type I and Type II performance requirements, although it is more stringent than that specified for Type I in the Operational Performance Requirements (OPR).

2.2.9 Unique Physical Characteristic.

The system must be based upon a unique physical biometric characteristic. This is a physiological feature that is basically unchanging and unalterable without significant trauma. Absent an accident or surgery, the original stored biometric data (template) should match biometric data captured years later. The biometric attribute must be certifiably unique to enable positive identification. Fingerprints, retina blood vessel patterns, and eye iris texture and features are examples of unique physical characteristics.

Some biometric IV systems are based upon characteristics classified as behavioral. Examples are signature, keystroke (typing) dynamics, and how one speaks (see paragraph 4.2.2 for further discussion). Because of behavioral variability over time, many of these systems update the reference template every time they are used. Generally, behavioral biometrics work best with regular use. Changes or distortions in behavior, as well as mimicking, introduce major shortcomings. For this project, user requirements limited candidates to systems based upon <u>unique</u> <u>physical</u> characteristics, not behavioral characteristics.

2.2.10 No Counterfeit Without Surgery.

Some biometric IV systems are vulnerable to defeat in various ways. For example, some fingerprint systems can be defeated by a "rubber finger" with a carefully created fingerprint. Some hand geometry systems can be defeated by a cast of a hand. A system which can only be defeated after surgical modifications affecting biometric characteristics is considered acceptably secure.

2.2.11 Decision Time.

The system must be capable of annunciating the accept/reject decision less than five seconds after the start of biometric data capture. This time period must include re-read times required by false reject decisions.

2.2.12 Visual/Audible Alignment Feedback.

The system must provide easily understood visual and/or audible feedback guidance for the entrant to enhance rapid and proper positioning, alignment or data collection.

2.2.13 Visual/Audible Accept/Reject.

The system must provide easily understood visual and/or audible annunciation of the accept or reject decision.

2.2.14 Easily Understood and Used.

The operation of the biometric equipment shall be easily understood so that no formal user training will be required.

2.2.15 Database of 40,000 Enrollees.

The system shall function as a stand-alone identification device, capable of verifying an individual's access authority. The system should handle a local database of up to 40,000 enrollees.

2.2.16 Integrates With A Central Database System.

The distributed capacity of the system when used in a multiple portal facility shall provide for connection of portal access verifiers to a central database for download of data and upload of events.

2.2.17 Integrates With Existing Military Systems.

The system shall be compatible with, and provide for an interface to, existing commercial and military-procured access control systems.

2.2.18 Enrollment Time.

The system shall permit initial enrollment verification in less than two minutes. This time period does not include entry of administrative data.

2.2.19 Operating Temperatures.

The system shall operate primarily in an indoor environment at temperatures from 0 to 65 degrees, centigrade (32 to 150 degrees, fahrenheit).

2.2.20 Operating Humidity.

The system shall operate in humidity conditions up to 95 percent, non-condensing.

2.2.21 Operable As An Exterior System.

The system shall not have intrinsic characteristics that, while initially operated indoors, will hinder future exterior installations.

2.2.22 System Mean Time Between Failures.

The system shall use concepts and equipment that will provide a high Mean Time Between Failures (MTBF). A MTBF of 10,000 hours (417 days of continuous operation) is a desired goal.

2.2.23 System Mean Time To Repair.

The system shall have a Mean Time to Repair (MTTR) of less than one hour.

2.2.24 Biometric Data Capture Unit Dimensions.

The biometrics information receiving assembly shall not exceed 24 inches by 24 inches by 12 inches in size.

2.2.25 Biometric Data Capture Unit Weight.

The biometrics information receiving assembly shall not weigh more than 30 pounds.

2.2.26 Single Portal Production Unit Cost.

Each single portal verifier shall have a production unit cost of $5,000 or less, as a goal.

2.2.27 Routine Preventive Maintenance Costs.

The system shall use concepts and equipment that will enable minimization of routine preventive maintenance costs.

2.3 OTHER DATA ELEMENTS IMPORTANT TO SYSTEM DEVELOPMENT DECISIONS.

2.3.1 No Active Input Required from Entrant.

Biometric IV system accuracy and effectiveness are impacted greatly by the data capture actions required of the entrant. In general, opportunities for error increase in relation to the amount of active input required from the entrants, even those desiring to be cooperative. Less than fully-cooperative personnel also produce higher error rates. Therefore, entrant-induced errors will be minimized in all cases if biometric data can be captured without active input from the entrant. The ultimate system would capture the necessary biometric data and identify the entrant who took no action other than to present himself at the portal.

2.3.2 User Concerns.

Society is increasingly impacted by perceptions of environmental health dangers and privacy issues. Recently, health concerns have focused on the Acquired Immune Deficiency Syndrome (AIDS), body fluids (including tears and saliva), contact with surfaces touched by many other people, and lights, rays, and electrical fields which invade the body. A growing area of user concern is the control and utilization of information acquired in the biometric data capture process. There have been cases where installed biometric access control systems could not be effectively utilized because of user concerns and reluctance (refusal) to use the devices.

2.3.3 Decision Time.

The user requirement (stated in Para. 2.2.11) is that the decision time must be less than five seconds in order to achieve desired portal throughput rates. However, the realities of human reaction time dictate that faster system operation times provide the best probability of meeting the desired throughput rates.

2.3.4 Size of Reference Template Required Per Individual File.

Larger data storage requirements result in higher system costs and in longer data search times, particularly for identification (vs. verification) systems. (Forty thousand 500-byte files require much less space than forty thousand 3,000-byte files -- 20 megabytes vs. 120 megabytes.)

2.3.5 Initial Procurement Cost For Smallest System.

The user requirement goal (stated in Para. 2.2.26) is that the one portal production unit cost must be less than $5,000. Obviously, a system that costs $3,000 per portal will be viable for more applications than a system costing $4,995. Also, an IV system capable of operating a single portal without an expensive CPU is much more flexible in application than a system always requiring a CPU, even if a CPU is added for multi-door applications.

2.3.6 Status Of The Product / Project.

What is the status of the product (if on the market) or the R&D project? Is the product on the (security) market, directed toward another market, in limited distribution, in (sales) trouble, or out of production? Is the project in early development (higher risk), mid-development, or late development?

2.3.7 Problems.

What are the problems or potential problems involved with utilization of this product or expected product? Can the biometric data capture process be perceived to be invasive? Do users consider the physical contact required for the data capture process to be onerous? Does this product have a significant user acceptance problem? Does a voice system have difficulty with background noise in either the enrollment or data capture processes? Does this system have an accuracy problem (Type I, Type II, or Crossover Error greater than three percent)? Does/will this facial recognition system have a problem handling faces rotated left/right or up/down, or changed expressions (happy, sad, excited, etc.), with or without glasses? No problems are identified in the requirements matrix (Appendix A) for those systems previously excluded by DNA assessment.

2.3.8 Qualified On Critical Criteria.

Does the system meet all the critical criteria?

Performs identity verification with no human in the operation/decision loop.
No physical contact with the entrant during the biometric data capture process.
Biometric data capture process is not invasive.
False rejection error rate is less than one percent.
False acceptance error rate is less than 0.1 percent.
Crossover Error rate is less than 0.1 percent.
Measures a unique physical biometric characteristic.

2.3.9 Development Potential Of The R&D Project.

What is the estimated development potential of the R&D project? These estimates will be explained in later discussions of the systems/technologies.

2.4 DATA COLLECTION MATRIX.

An example of the matrix utilized in collecting data for this project is shown below.

SAMPLE

PERFORMANCE, OPERATIONAL & TECHNICAL REQUIREMENTS MATRIX

	SYSTEM REQUIREMENTS	SYSTEM A	SYSTEM B
1	**USER:**		
2	PERFORMS VERIFICATION		
3	PERFORMS IDENTIFICATION		
4	NO MAN IN THE LOOP		
5	NO CONTACT		
6	NON-INVASIVE		
7	TYPE I FALSE REJECT < 1 %		
8	TYPE II FALSE ACCEPT < 0.1 %		
9	TYPE I -TYPE II CROSSOVER POINT		
10	UNIQUE PHYSICAL CHARACTERISTIC		
11	NO COUNTERFEIT W/O SURGERY		
12	DECISION TIME < 5 SEC		
13	VISUAL/AUDIBLE ALIGNMENT FEEDBACK		
14	VISUAL/AUDIBLE ACCEPT/REJECT		
15	EASILY UNDERSTOOD / USED		
16	STANDALONE DATABASE OF 40,000		
17	INTEGRATES W/ CENTRAL DATABASE		
18	INTEGRATES W/ EXISTING MIL SYSTEMS		
19	ENROLLMENT < 2 MIN		
20	OPERATING TEMP 32-150 DEGREES F		
21	OPERATING HUMIDITY 0-95%		
22	OPERABLE AS EXTERIOR SYSTEM		
23	M T B F GOAL 10,000 HOURS (417 DAYS)		
24	M T T REPAIR < 1 HOUR		
25	SIZE < 24"X24"X12"		
26	WEIGHT < 30 LBS		
27	ONE PORTAL PROD UNIT COST < $5000		
28	MAINTENANCE COST		
29	**OTHER:**		
30	NO ACTIVE INPUT		
31	USER CONCERNS		
32	ACQUIRE & DECISION SPEED		
33	INDIVIDUAL DATA STORAGE SPACE - BYTES		
34	INITIAL COST - SMALLEST SYSTEM		
35	STATUS:		
36	PROBLEMS:		
37			
38			
39	QUALIFIED ON CRITICAL CRITERIA :		
40	DEVELOPMENT POTENTIAL:		

SECTION 3

RESULTS OF RESEARCH EFFORTS

3.1 SOURCES OF INFORMATION.

3.1.1 Government Repositories.

Two government information repositories were researched: The National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA, and The Defense Technical Information Center (DTIC), Building 5, Cameron Station, Alexandria, VA. The NTIS database search revealed about 8,000 titles which included one or more of the key words/phrases. Abstracts of over 120 articles or documents were reviewed. Eleven documents were obtained from NTIS. The DTIC search identified 30 documents for which abstracts were provided. Seven were of interest, six of which had been obtained from NTIS. Only one additional document was obtained as a result of the DTIC search. All twelve documents are listed in SECTION 6, REFERENCES.

3.1.2 Industry Periodicals.

Information for this project was obtained from the following industry periodicals.

a. *Personal Identification News (PIN)*; Ben Miller, Editor; Warfel & Miller, Inc, Publisher.

b. *Biometric Technology Today*; Emma Newham, Editor; SJB Services, Publisher.

c. *Special Technologies*; Ken C. York, Editor; American Pioneer Technologies, Inc., Publisher.

d. *Security Technology News*; Candace D. Sams, Editor; Phillips Business Information, Inc., Publisher.

e. *Access Control*; Gregg Echols, Editor; Argus Business, Publisher.

f. *Automatic I. D. News*; Mark David, Editor; Advanstar Communications, Inc., Publisher.

g. *International Fire and Security Product News*; Colin W. Bridges, Editor; Paramount Publishing Limited, Publisher.

h. *I D Systems*; Deborah Navas, Editor; Helmers Publishing, Inc., Publisher.

i. *Security Dealer*; Susan A. Brady, Editor; PTN Publishing Company, Publisher.

j. *Security*; Bill Zalud, Editor; Cahners Publishing Company, Publisher.

k. *Security Management*; Mary A. Crawford, Editor; American Society for Industrial Security, Publisher.

3.1.3 Personal Information Sources.

All IriScan personnel involved with this project collected information on biometric identification R&D projects from personal contacts in the industry. Information on projects identified was then verified by official reports or by those conducting the research.

3.1.4 Sandia National Laboratories (SNL) Reports.

a. *The Status of Personnel Identity Verifiers*, July 1985

b. *A Performance Evaluation of Biometric Identification Devices*, June 1991

c. *Intelligent Facial Recognition Systems*, September 1993

d. *A Performance Evaluation of Biometric Identification Devices*, 1993 (A verbal report of the 1993 tests, presented by Jose Rodriguez, Entry Control Program Head, SNL, at the October 27, 1993, Inter-agency RDT&E Technical Seminar at Scott Hall, Fort Belvoir. The written report has been submitted for publication and is expected to be dated June 1994.)

3.1.5 *Commerce Business Daily (CBD)*, Superintendent of Documents, Government Printing Office, Publisher.

3.2 OTHER SYSTEMS.

While the investigation and attempts to identify every applicable IV system were exhaustive, some engineering development projects and agencies were excluded from the study. In those cases where DNA was familiar with the project/effort (e.g., Central Intelligence Agency (CIA) facial recognition, Los Alamos National Laboratory (LANL), and National Security Agency (NSA) iris recognition projects), it was not deemed necessary to repeat that information.

3.3 DATA COLLECTION AND ORGANIZATION.

a. The first data entered in the Performance, Operational & Technical Requirements Matrix was extracted from SNL Test Reports. In general, these reports provide the most complete and reliable information available on those systems SNL has tested. Systems which have been tested by SNL are designated in the Matrix by asterisks (*) on Line 1 and Line 29.

b. Data from other unbiased tests and evaluations was entered into the Matrix next. Primarily, this data came from Thesis Reports of students at the Naval Post Graduate School. Systems reported in this category are designated in the Matrix by plus signs (+) on Line 1 and Line 29.

c. System/R&D project data from all other sources was then entered into the Matrix as it was obtained. The data was then organized in two ways. First, systems which had reached the marketplace were separated from those still in development. Then, each group was organized by technology, i.e., eye, voice, hand/finger, signature, keystroke, and facial recognition. See Appendix A, Performance, Operational & Technical Requirements Matrix. Page A-1 includes all of the Marketplace Systems, while the Research and Development Systems are on page A-2. The Item Notes on Page A-3 provide convenient descriptions of the data elements of the Matrix. Page A-4 contains available address, telephone, fax and point-of-contact information on the systems and projects addressed in the Matrix.

SECTION 4

ANALYSIS OF DATA

4.1 CRITICAL CRITERIA SCREENING OF MARKET SYSTEMS.

4.1.1 Although all available data on each system/project was entered into the Matrix, the first "screening" was based only upon the criteria which are considered critical. Systems which do not meet any one of the critical criteria were eliminated from further evaluation. Since this decision was so vital, only systems whose capabilities have been established in operational use were subjected to this screening. (See Appendix A, Performance, Operational, & Technical Requirements Matrix, Page A-3, Market Systems.)

4.1.2 All of the systems currently in the marketplace were eliminated. In each case, at least one of the critical criteria was not met.

a. EyeDentify was eliminated for several reasons. First, current configurations require contact with the system to complete data capture. Second, the low-power infrared beam which penetrates the pupil to illuminate and scan the retina is considered invasive. Third, although the SNL tests of 1991 indicated that EyeDentify's Crossover Error Rate (CER) performance was much improved over the 1985 SNL tests, the CER is still 1.5%. This is significantly short of the 0.1% derived from the SOW. User resistance resulting from disease and eye injury concerns has greatly limited utilization of this technology. EyeDentify's efforts to develop a non-contact model do not substantially alter the nature of the invasive process described above.

b. Voice Strategies was eliminated for several reasons. Contact with the equipment is required to initiate the process and input the PIN. Secondly, the 1993 SNL Test (reported by Jose Rodriguez at the Inter-agency RDT&E Technology Seminar) resulted in a Crossover Error Rate of 28%. The system is a verifier only, and can not identify the would-be entrants. And finally, the uniqueness of voices has not been established, nor is it a physical biometric characteristic. It is, in reality, a behavioral characteristic. (See Par 4.2.2, below, for discussion of voice systems in general.)

c. The Alpha Microsystems Ver-A-Tel is out of production. Contact was required to input the PIN. The Type I and Type II error rates did not meet the standard (as reported by the 1991 SNL test). System decision time was also greater than five seconds. Additionally, the system verifies only and measures a behavioral characteristic, not a physical characteristic.

d. The International Electronics (ECCO) VoiceKey is in limited distribution under special sales conditions. The system requires contact to input the PIN. The Type I, Type II, and Crossover Error Rates did not meet the standard (as reported by the 1991 SNL test). This system, which utilizes a wall-mounted microphone, could possibly be modified with an IR sensor as a sequence initiator to become a no-contact system. However, the system is very sensitive to the position of the mouth in relation to the microphone. Consequently, the modified system is not likely to be able to achieve the required error rates because it would still have the background noise problem so debilitating to voice systems. Additionally, the system verifies only and measures a behavioral characteristic.

e. The ITT SpeakerKey is currently used in the house-arrest verification and telephone system security fields. If applied in the access control field, the same disqualifying performance facts inherent in other voice systems are present. The system utilizes a telephone handset as an input device, requiring contact. The Crossover Error Rate reported by ITT is 2.2%. Finally, voice IV is not based on a unique physical biometric characteristic, but rather, a behavioral characteristic.

f. The Ensigma voice system was part of the 1993 SNL test. The system utilizes a PIN and a telephone handset as input devices, requiring contact. The

Crossover Error Rate is 16%. The system verifies, rather than identifies, and measures a behavioral characteristic.

g. Recognition Systems' Hand Geometry was included in both the 1991 and 1993 SNL tests, as well as a thesis evaluation. The system requires a PIN and physical contact for data capture. Though the system achieved a Crossover Error Rate of 0.2% on the 1991 test, its performance had dropped to 3% on the 1993 test. It is also known that counterfeit hands can be used successfully, under certain conditions. This system is only able to verify identity.

h. The Palmguard palmprint system described in the 1985 SNL report requires contact and is considered invasive. It did not meet the Type I or Type II Error Rate standards, and the system is not in production.

i. The Stellar Identimat finger length verifier also described in the 1985 SNL report required contact, is considered invasive, and did not meet the Type I or Type II Error Rate standards. Additionally, this system is out of production.

j. The Identix TouchLock (fingerprint) system utilizes a card reader for PIN input and requires physical contact for data capture. The system was part of the 1991 and 1993 SNL tests. The latest known Crossover Error Rate is 5%. Counterfeit fingers can be used successfully, under certain conditions.

k. The Transaction Systems, Ltd., signature dynamics verifier tested for the 1985 SNL report required contact and did not come close to meeting False Rejection and False Acceptance standards. This British system is not on current production lists and its present status is unknown. Verification is based on a behavioral characteristic.

l. The Capital Security Systems Auto-Sig system requires contact for data capture, as well as a card swipe for the PIN. As reported by the 1991 SNL test, neither the Type I or Type II Errors meet the required standard. A Crossover Error Rate was not calculated. It has not been demonstrated in the identification mode and it does not measure a unique physical biometric characteristic.

m. The Xenetex Signature Dynamics system was part of the 1993 SNL test. Contact is required for data capture. The Crossover Error Rate was 17%. The system does not measure a unique physical biometric characteristic.

n. The Communication Intelligence Corporation (CIC) On-Line signature dynamics system underwent a ten-week, 24 person, thesis evaluation. Contact is required for data capture, both in printing the PIN and writing the signature. Even in this limited test, the system did not meet the False Rejection or False Acceptance standards. Additionally, this system does not measure a unique physical biometric characteristic.

o. The Capital Security Systems Sign/On requires contact for data capture, as well as typing the PIN. The ten-week, 24 person, thesis evaluation resulted in Type I and Type II Errors which did not meet the standard. This system is only able to verify a behavioral characteristic.

p. The Phoenix International Software BioLock keystroke dynamics system requires contact in typing the PIN and the prompted words. The three-month, 24 person, thesis evaluation resulted in Type I and Type II errors which did not meet the standard. This system is only able to verify a behavioral characteristic.

q. The NeuroMetric Vision Systems Facial Recognition System was evaluated at SNL during the 1993 Intelligent Facial Recognition Systems evaluation. This study concludes that, "Semi-automatic applications in an environment in which a selection of a few faces are given as a possible match for the face to be identified should be in place within a year or two with little or no error. In these applications, the final decision is made by a human operator." This "man-in-the-loop" is a critical disqualifier, as is the fact that the human face cannot be established as certifiably unique. (See Par 4.2.3, below, for further discussion of facial recognition systems in general.)

4.2 TECHNOLOGY ANALYSIS OF DEVELOPMENT PROJECTS.

4.2.1 General.

The Development Projects/Systems which were identified fall into three categories. These are voice recognition, facial recognition, and iris recognition.

4.2.2 Voice Recognition Technology.

As a class, voice recognition systems do not verify on a unique physical characteristic. They verify based upon a behavioral characterist. While not commonly considered behavioral, the voice would seem to meet the criteria Ben Miller has offered in references 14 and 15. Physical characteristics are "...basically unchanging and unalterable without significant duress." Voices, in contrast, change with age, psychological or emotional state, microphone orientation, and health. Although limited by physical parameters (size of lungs, esophagus, vocal cords, mouth, etc.) most people can alter their voice over a wide range of volume, pitch, resonance, and other measurements. Trained voices can span several octaves.

In general, voice recognition systems attempt only to verify identity of individuals. Of the eight systems reviewed (five on the market, and three in R&D), only the AUM System's independent text voice verification system claims to identify as well as verify. Inability to obtain technical information however, prevents comment on its effectiveness in that regard.

Voice systems historically have suffered from ambient noise problems (References 12 through 15). For example, experience at the September 1993 ASIS exhibits was that, even with a telephone handset in use in place of a free-standing microphone, repeated attempts were necessary in order to enroll. This may be the reason that Crossover Error Rates for the marketed systems vary from 2.2% (company calculation) to 28% (SNL test). A lack of available technical data for the systems in R&D prevents objective comment on their effectiveness. The Type I and Type II error rates of 9.5% and 17% from the SNL test of the LANL R&D system, however, do not portend a promising trend.

Voice systems do not, at first consideration, present a problem of intrusiveness or invasiveness. Because of the ambient noise problems mentioned earlier, however, handsets have, in some cases, been substituted for microphones which, of course, requires contact and may also be judged as intrusive. The most prominent voice system in the marketplace today, for example, requires the user to pick up a handset, enter a four-digit PIN, and then put his mouth against the mouthpiece of the handset to speak. Considering that users with colds, diseases, and varying amounts of saliva on their lips, could precede one through a portal, system use will appear intrusive or, at least, unpalatable and unacceptable.

4.2.3 Facial Recognition Technology.

Facial recognition, and particularly automated facial recognition, has been the target of compelling pursuit for years. As the authors of the Los Alamos report, *Back Propagation Neural Networks for Facial Recognition* (LA-12353), October 1992, point out, Bertillon (1853-1914) was studying this issue before the turn of the century. The problems inherent in facial recognition have been acknowledged in the past, and until recently, have deterred mainstream research organizations from exploration. Dramatic increases in computing power and speed have contributed to new efforts to develop facial recognition/verification into a practical system. Nearly 78% of the candidate R&D systems reviewed, for example, dealt with facial IV. Fourteen of the eighteen systems currently in R&D were based on facial recognition or verification.

The problems encountered by early investigators in facial IV were, in fact, real and valid, independent of computing power, and remain so today (References 3 and 17). The basic fact that the human face is <u>not</u> unique (National Organization of Mothers of Twins Clubs publication 8-93/LKD/15000) should be adequate reason to pursue other, more fruitful, areas of investigation. It seems, howeve, that this issue is largely ignored by investigators. This may be partially based on the attractive link with photographic/video availability of facial images.

In addition to the inherent fact that the human face is not unique, changing the appearance of the face is a simple and obvious act that has been practiced for thousands of years. The ability to masquerade or surgically alter a facial feature has become an art or craft capable of incredible transformations. The fact that there were approximately 31,288 identical twin births in 1990 (same reference as above) should also concern facial biometric developers.

Finally, despite the progress in computing power, automated facial recognition remains elusive and has been recognized by authorities in the field as an impractical goal. The pr ously referenced Los Alamos report is quoted, as follows:

> "Face recognition is impractical for a large population because of the number of individuals that the network would be required to learn. In addition, inclusion of a new person to the population would require the network to relearn all the people in the population. Learning is a slow process, and relearning is clearly desirable."

As apparent corroboration of this conclusion, only three of the fourteen facial "recognition" R&D projects being pursued today, claim to be able, or have as a goal, to recognize individuals by identification, rather than verification. The remaining eleven projects claim only to be pursuing systems capable of verifying individual identity with the use of a PIN or card. SNL's Cynthia Nelson, in the September 1993 report, *Intelligent Facial Recognition Systems*, concluded that systems may be available in a year or two that may operate with "little or no error," but all will require a human operator to make the final judgement. In addition, she concluded that, "If a person is aware of the presence of a recognition system and does not wish to be recognized, it is believed that (s)he could easily spoof any fully automatic system that bases decisions solely on facial information."

4.2.4 Iris Recognition Technology.

Because the IriScan technology/system is described in great detail in SECTION 5, CONCLUSIONS, it will not be reported here.

4.3 CRITICAL CRITERIA SCREENING OF DEVELOPMENT PROJECTS.

Since all of the R&D projects are still in the development stage, there is little information about any of these potential systems which can be positively verified at this time. In some cases, strong inferences can be drawn, based upon the stated utilization of the system. In other instances, system information is drawn from scientific papers presented by the developers.

4.3.1 Voice Recognition Technology.

a. Sonetech's independent-text voice verification system was described in a proposal to the government. Systems which permit the entrant to speak any (random) words, as opposed to specific, cued, and enrolled words, will represent a significant step in voice recognition, if proven successful. However, this achievement may also aid imposter/counterfeiters, since they need not be ready to instantly present unknown, or unexpected words. DNA's knowledge of the system resulted in direction that no extensive effort/analysis be directed toward this system. This caused the "NA" to be entered on the Development Potential line of the matrix. Regardless of random word comparison, the system is behavioral and is susceptible to the deficiencies which limit all voice systems. It was eliminated.

b. AUM Systems' independent-text voice verification system was introduced by the Immigration & Naturalization Service (INS), which had received a demonstration.

AUM requested that IriScan investigators visit their laboratory in northern New Jersey for a demonstration. However, after AUM presented a demonstration at DNA, they no longer responded to telephone or fax communications from IriScan. Based upon the developer's statements, the system operates as an identifier, correct more than 99% of the time. The entrant presents five seconds of speech (probably reducible to four seconds or less), and the decision time with a 150 person database is about one-half second. AUM was starting to study false accepts, but did not understand Type I Error, Type II Error, or Crossover Error Rate. They claim that every voice recorder/player has magnetic heads which create noise at specific frequencies. Their system will scan these frequencies to ensure that they have a live person speaking. Utilization of CDs and records was not discussed. (Apparently, at DNA, the statement was that the motor driving record, CD, and tape players generated the noise, which AUM could detect.) Enrollment requires 3 - 15 seconds of speech input. AUM's approach to voice recognition is believed to be innovative and they have the only voice system which purports to do full recognition. It is too early in the development cycle to make definitive statements about potential system effectiveness; however, there is no reason to believe that AUM will not be affected by the background noise problem which results in unacceptable Type I, Type II, and Crossover Error rates for all of the voice systems which SNL has tested. It was eliminated for this reason.

c. Los Alamos National Laboratory's voice system was evaluated in the 1985 SNL test report. Enrollment time averaged 3.4 minutes per person. Average verification time was about 18 seconds. The False Rejection rate was about 9.5% and the False Acceptance rate was about 17.7%. Though the system was thought to be less affected by background noise than some other voice systems, the performance factors are so far short of the acceptable standards that the system was eliminated.

4.3.2 Facial Recognition Technology.

a. The facial recognition technologies, and methodologies which follow were eliminated from further serious consideration for several reasons. They are not based on unique physical biometric characteristics, there are numerous counterfeiting techniques known and effectively practiced, and SNL has concluded that facial systems are easily spoofed. (See paragraph 4.2.3, above, for a further discussion of facial recognition technology in general.) Where are additional reasons for elimination of specific methodologies or systems, they are noted.

b. The Massachusetts Institute of Technology (MIT) Eigenfaces system is discussed in the SNL 1993 Intelligent Facial Recognition Systems report, and it has also been previously studied by an IriScan scientist. IriScan's chief scientist, Dr. John Daugman, of Cambridge (England) University, is an editor of four scientific journals and has reviewed Eigenfaces papers submitted for publication. SNL reports (reference 17), "...eigenfaces are the set of orthonormal basis vectors providing optimum approximation for a collection of the face images in the sense of minimum mean-square error." Dr. Daugman concurs that the idea is to represent any possible face as a linear combination (i.e., a weighted average) of some set of (roughly 20) functions, or eigenfaces. However, faces are neither linear nor two-dimensional. Application of this approach to a database of about 7,800 is said to have achieved an accuracy rate of about 95%. The Eigenface facial recognition verification system was described in a government proposal. Low accuracy also contributed to eliminate this system.

c. Arial's facial recognition verification system was described in a proposal to the government.

d. The Mikos Ltd. facial thermography verification system was described in a proposal to the government. This system was also discussed in the SNL 1993 Intelligent Facial Recognition Systems Report. In addition to the comments of paragraph 4.3.2 a., above, high expected system cost, contributed to elimination of this system.

e. The Information Systems Network (ISN) facial recognition system was described in a proposal to the government.

f. The A. C. Nielsen facial recognition system, being developed in conjunction with Bell Laboratories, is an attempt to produce a system which will provide continuous positive identification of previously enrolled persons sitting in front of a television set. Nielsen/Bell have treated this project very discretely, and refuse to discuss it now. The little information available indicates that about $9 million has been spent, but without known success. Recognition of multiple, moving faces is extraordinarily difficult. Indeed, recognition of one still countenance has not been achieved on an acceptable basis. There are no indications that Nielsen/Bell has been successful in this effort.

g. The David Sarnoff Research Center's system is discussed in the SNL 1993 Intelligent Facial Recognition Systems report. This system is being designed for initial, and continuous, computer terminal access control. The system is stated to have been demonstrated with some limited success. It is believed that terminal access would be limited to only a few persons (small database).

h. The E-Metrics (subsidiary of General Dynamics) system is discussed in the SNL 1993 Intelligent Facial Recognition Systems report.

i. The Physical Optics system is discussed in the SNL 1993 Intelligent Facial Recognition Systems report. This is a three-layer, neural network system that has been trained on multiple images of eleven people. The lengthy "training" required to achieve a effective neural network system would result in enrollment times far greater than the standard.

j. The SD-SCICON system is discussed in the SNL 1993 Intelligent Facial Recognition Systems report. This is a neural network system that has been trained on 40 seconds of video on each person. The recognition decision is displayed as a bar chart ranking of each person in the database according to how well that person matches the person being identified. The lengthy "training" required to achieve an effective neural network system would result in enrollment times far greater than the standard.

k. The University of Illinois recently signed a contract with the Army Research Laboratory (ARL) to perform research and development of face recognition algorithms. This is in support of a DARPA project called Faces in the Crowd, intended to perform automated identification of police "mug shots" and individuals in photos or videos of crowds.

l. The Analytical Sciences Corporation (TASC) recently signed a contract with ARL to perform research and development of face recognition algorithms (Faces in the Crowd).

m. The University of Southern California recently signed a contract with ARL to perform research and development of face recognition algorithms (Faces in the Crowd).

n. Rutgers University recently signed a contract with ARL to perform research and development of face recognition algorithms (Faces in the Crowd).

4.3.3 Iris Recognition Technology.

IriScan, Inc., is developing an IV system based upon the fact that the iris of each human eye is unique, even in the same person and between identical twins. This system has been demonstrated in the laboratory/prototype setting, but it has not been evaluated by SNL. Indications are that it has a good probability of meeting the standards required of the DoD biometric access control system. The specifics of this system will be covered in the next section.

SECTION 5

CONCLUSIONS

5.1 GENERAL CONCLUSION.

The research undertaken for this project found no system, technology, or methodology which can currently meet all of the objectives and the Operational Performance Requirements specified in the Statement of Work. Of the systems, technologies, and methodologies under development, only the IriScan system of positive identification/verification using an iris recognition process appears capable, with further development, of meeting those objectives and requirements. Based on our research, the primary alternatives of voice and facial recognition cannot now, or in the foreseeable future, meet many of the stringent requirements for DoD application. Their inherent inability to satisfy critical criteria cannot in the immediate future be overcome by additional cost effective development.

5.2 QUALIFICATION OF THE IRISCAN SYSTEM.

5.2.1 General.

We have attempted in this report to clearly distinguish between the data available on systems and technologies which have been tested by an outside agency and similar data on systems which have not been independently tested. In the former case, (given that one accepts the validity of the experimental paradigm) the data would appear to be more reliable. In the latter case, one is forced to rely on vendor statements and/or theoretical but unproven data. Clearly, statements about the qualification of the iris identification technology proposed by IriScan falls into the second category. Many of the conclusions and much of the quantitative data provided below, however, have been demonstrated in operating laboratory models, and/or are accurately extrapolated based on data developed through the R&D of those models, or are based on rigorous and verifiable mathematical and scientific principals. Many of the standard requirements (such as operating temperature, humidity, MTBF, MTTR, size, weight, etc) are so well within the capabilities of component state of the art, that we have concluded that the IriScan system/technology is "capable with further development" of meeting the requirement, even though that fact cannot be fully demonstrated until development is complete.

5.2.2 Qualification IAW Performance, Operational, and Technical Requirements Matrix.

5.2.2.1 Performs Verification. Current software and hardware being utilized in the laboratory models provide only identification, not verification. However, verification is an easier task and therefore should be readily achieved in development. The improvement in decision speed by pre-identifying a file is unknown, although it is theorized that it will be minimal in a small database.

5.2.2.2 Performs Identification. Meets requirement. The current laboratory model was designed to, and is currently operating in the identification mode.

5.2.2.3 No Man in Loop. Meets requirement. System in the "Live Recognition" mode is fully automated.

5.2.2.4 No Contact. Meets requirement with two caveats. Operation in the verification mode will force a user to contact the system, traditionally by entering a PIN or swiping a card. In the identification mode, contact is not required unless the image acquisition component must be manually adjusted to accommodate a specific user application. A generic user interface has not yet been defined, but could result in a standard, automated approach to all users. One option being considered is that of a fixed, angled screen, much like those encountered at ATMs. This configuration would not require contact, but might require some physical body movement to bring the eye into proper alignment.

5.2.2.5 Non-Invasive. Meets requirement. Technology only requires a video/photo image of the eye.

5.2.2.6 Type I Error Rate < 1%. Meets requirement. Current False Reject rate with Hamming Distance criteria set at .32, is 1 in 128000, or .00078% (Reference 5).

5.2.2.7 Type II Error Rate < .1%. Meets requirement. Current False Accept rate with Hamming Distance Criteria set at .32, is 1 in 151,000, or .00066% (Reference 5).

5.2.2.8 Crossover Error Rate (CER). An Operational Performance Requirement was not specified. The IriScan crossover error rate of .00076%, however, is nearly 2,000 times lower than any CER tested or claimed by any biometric system (Reference 5).

5.2.2.9 Verifies on Unique Physical Characteristic. Meets requirement. The iris of the eye is known to be a stable physical characteristic which does not change between the ages of twelve months and about eighty years. Additionally, quoting Dr. John Daugman (Reference 5) as follows:

> An advantage the iris shares with fingerprints is the chaotic morphogenesis of its minutiae. The iris texture has chaotic dimension because its details depend upon initial conditions in embryonic genetic expression; yet the limitation of partial genetic penetrance (beyond expression of form, function, color and general textural quality), ensures that even identical twins have uncorrelated iris minutiae. Thus the uniqueness of every iris, including the pair possessed by one individual parallels the uniqueness of every fingerprint, regardless of whether there is a common genome.

5.2.2.10 No Known Counterfeiting Technique. Meets requirement. There is a caveat in that an intensive investigation of spoofing techniques has not been accomplished on the system. Apparent techniques to counterfeit the structure of the iris, specifically: surgery, contact lens, and photos of the iris do not appear to be viable. Surgery cannot be undertaken without great risk to sight and is a highly unlikely method to attempt to copy an iris. Contact lens and photographs are countered by algorithms inherent in the IriScan software. These algorithms, among other features, check for pupillary unrest (commonly, although erroneously called "Hippus" movement) which is continuous, unconscious, and independent of will. Absent Hippus movement, the IriScan system will consider the image as artifice and will not make an identification/verification.

5.2.2.11 Throughput Rate: Decision Time < 5 sec. Meets requirement with caveat.

a. Currently the IriScan laboratory model will make a decision to identify approximately 1.5 seconds after acquisition of an acceptable iris image. Since there are no provisions for verification, no statement can be made with regard to decision time in that mode although it is reasonable to assume that, with a large database, the time would be shortened in the verification mode. There are also no provisions for making a decision to reject. The system merely continues to acquire images and to rescan the database for a match. A software modification will be required to provide this capability.

b. It is useful when considering the issues of "retries" and decision time, to consider the activities which occur in the iris identification process. The video frame grabber "grabs" frames when processing (currently at the approximate rate of one per second...ultimately, at the standard video rate of 20 to 30 per second). The system views the frame for focus, size, "eyeness", and other factors to ascertain quality of the image. If the frame meets certain standards and is of sufficient quality to be useable, processing begins/continues. If not, the system continues to grab frames until it finds one of sufficient quality. In a sense, it has already "retried" the biometric sampling before further processing in order to assure itself of an adequate image. If an adequate image is found, it is converted to an iriscode. It compares the selected iriscode with every file iriscode sequentially to find a match. If none is found, it re-compares with each stored iriscode, rotating the sample plus (+) and then minus (-) two degrees to compensate for possible head tilt (rotation). If no match is found, it re-compares with each file iriscode, rotating the sample +/- 4 degrees. The process is continued, incrementing an additional 2 degrees each time until the maximum allowed by the current software of +/- 16 degrees is reached. A software option can be selected by keystroke to increase this compensation for head tilt to a maximum of +/- 84 degrees, however current use of this option has been limited to demonstration only. Thus the process involves multiple retries, in both the biometric sampling, and more dramatically, in the matching process.

c. This inherent retry feature can extend the decision time, especially if the expanded recognition option is invoked, and the authentic entrant has the head rotated radically. In practice, the decision time of 1.5 seconds is routinely achieved with head rotations of 5 - 7 degrees. Further, data from thousands of identification trials indicates that normal head tilt does not exceed +/- 10 degrees.

d. The implications of the iris processing as described above are profound ... at least from a theoretical standpoint. First, some decision point must be established to create a "rejection". The point at which the system completes its + and - 16 degree comparison without a match, seems like a logical one. Secondly (and again, theoretically since we have not yet completed even the brassboard unit), a rejection following the extensive comparisons described above means that either the entrant is deliberately trying to be obtuse with the system, or (more likely) the individual is really <u>not</u> in the database and is, therefore, an imposter.

5.2.2.12 <u>Visual/Audible Feedback for Alignment</u>. Meets requirement. Although subject to reconfiguration during further development, the system provides liquid crystal display (LCD) feedback with a cross hair for alignment.

5.2.2.13 <u>Visual/Audible Feedback for Accept/Reject</u>. Meets the "accept" requirement. Capable of meeting reject requirement with simple software change. Currently, for R&D purposes, the IriScan system announces the individual's name, which eye, and the imposter odds, when it makes an identification. This will be refined during development to a more user-oriented function such as activating a strike and/or light. A visual/audible reject feedback mechanism will be incorporated with the implementation of the reject decision function.

5.2.2.14 Easily Understood/Used. Meets requirement. Informal instructions to users are simple, easily implemented, and have always resulted in image acquisition.

5.2.2.15 Local Database of 40,000. Capable, with further development. Although development has required only several hundred iriscodes/files in the system to date, 40,000 is readily achievable.

5.2.2.16 Integrates with Existing Database. Capable, with further development.

5.2.2.17 Integrates with Military Systems. Capable, with further design.

5.2.2.18 Enrollment Time < 2 minutes. Meets requirement. Current enrollments can be accomplished in less than one minute.

5.2.2.19 Operating Temperature 32-150 Degrees F. Capable, with further development.

5.2.2.20 Operating Humidity 0-95%. Capable, with further development.

5.2.2.21 Operable as Exterior System. Capable, with further development.

5.2.2.22 MTBF Goal 10,000 Hours. Capable, with further development.

5.2.2.23 MTT Repair < 1 Hour. Capable, with further development.

5.2.2.24 Size < 24x24x12. Capable, through standard development.

5.2.2.25 Weight < 30 lbs. Capable, through standard development.

5.2.2.26 One Portal Production Cost < $5,000. Capable, with qualification. Target cost will be less if constructed to "Best Commercial Standards". If ultimate production must be to MILSPEC, it will drive costs much higher, and an accurate estimate is not possible at this stage of R&D. Likewise, if the ultimate user imposes requirements or functions beyond the Operational Performance Requirements of the SOW, this conclusion may be invalid.

5.2.2.27 Maintenance Cost. Expected to be low since the data acquisition module is expected to have no moving parts and entrants are not expected to have physical contact with the system.

5.3 SUMMARY OF DEVELOPMENT DECISION INFORMATION.

5.3.1 Support System Requirements (Appendix B).

Appendix B details Support System requirements for several optional system configurations (single portal, multiple portal, and complete system) as though it were a stand-alone system, that is, not integrated with any other entry/access control system. For the purpose of this developmental effort, as well as for this summary, it is useful to make a dual assumption:

> If development of an iris-based biometric identifier verifier (IV) is continued, it will conceptually be an add-on to the Air Force-developed AECS, just beginning deployment to the field. It need not, therefore, be designed and developed as a totally independent, stand-alone system.

Under this assumption, nearly all of the Support System requirements detailed in Appendix B will already be met by the design provisions of the AECS. Even under that scenario, however, there are some support requirements which should be addressed at this stage of development.

Conceptually, the IriScan IV could be deployed in the role envisioned for the Personal Identity Verifier (PIV) in the Level III installations of the AECS. Optionally, however, given its potential, it could substitute for either or both the PIN and the magnetic stripe card (MSC) in Level III installations. Potentially, it could also be used in Level II and Level I installations as well, eliminating the need for cards, readers, and PINs entirely.

The Support System requirements would vary depending on the role which the IV system assumes. Given that it acts only as the PIV in Level III systems, the output of the IriScan reader would be an IriScan file number which might then have to be translated by the software of the AECS (via a look-up table, probably) to the file number of the individual's card and PIN. Additionally, the "and" logic of the AECS decision software (which now presumably requires the file number from card and PIN to agree) might have to be modified to include this new, third input. If the IriScan biometric were used as a substitute for one or the other of the two identifiers (PIN or card), however, the look-up table might be incorporated into the software of the IriScan biometric device so that its output would be identical to the currently specified output of whichever device it is substituted for. If the IriScan biometric device replaced both the card and PIN, the IriScan look-up table might be required, and the software of the AECS might require modification to eliminate the "and" logic entirely.

5.3.2 Technical System Requirements (Appendix C).

The purpose of the Technical System (portion of the total IriScan system) is to positively identify a would-be entrant at a portal. It must provide the following functions to accomplish the:

a. Visual/audible feedback to assist the entrant in alignment.

b. Video capture of the iris characteristics.

c. Digitizing and processing of the video information.

d. Comparison of the captured, digitized, and processed image with iriscodes stored in a database.

e. Identification of the would-be entrant.

f. Output of a file identifier to the Support System for a decision on entry and for activation of the strike.

It will be comprised of two major components, the Image Acquisition Module (IAM) and the Computational Platform (CP). The IAM will accommodate individuals of varying heights, provide for alignment feedback, and provide illumination necessary to the process. The CP digitizes, processes, and compares the iriscode of the acquired image with the iriscodes filed in the database and identifies the individual by file number. It will communicate with the Support System as necessary to complete the entry control process.

5.3.3 Operational Scenarios (Appendix D).

Enrollment can occur either at the portal, in the case of a stand-alone or small multi-portal system, or at a centralized location in a larger system. Enrollment will require the active participation of a system operator. Enrollment involves positioning and alignment (currently), focus, activation, and validation.

Portal entry can be a[illegible]orized in the identification mode where the entrant merely aligns the eye and the system recognizes him/her, or in the verification mode, requiring the entrant to also present a card or PIN.

In the standard configuration, exit from an area requires no further interface with the system. In the Personnel Tracking configuration, an individual must interface with the system upon exiting, c[illegible]ent[illegible] any area will not be allowed.

5.3.4 Estimate of Remaining Development Costs (Appendix E).

Appendix E provides the estimated detail of costs to complete the brassboard, proof-of-principal phase.

Estimating costs beyond the brassboard phase is much more difficult because there are many factors which could have dramatic effects on any developmental program and hence costs. What will be the ultimate configuration of the units and the "system"? Will "Best Commercial Standards" be adequate, or will the system be "MILSPEC'd"? Will the ultimate user demand features beyond those inherent in the brassboard? Will a requirement for one or more additional features require extensive engineering development as opposed to the concept outlined in Appendix I, Strawman Deployment POA&M? Will a decision be made to use an iris-based biometric device in other than Level III installations?

These are only a few of the many variables which can materially alter any estimate for production made at this point in development. Given that qualification, we can offer rough order of magnitude estimates only at this time.

If the concept, timing, and quantities remain as outlined in Appendix I, and given that the requirements do not change from those in the current SOW, we would expect that the cost to develop an IriScan "system" capable of fulfilling would not exceed $900,000.

5.3.5 Estimate of Core System Costs (Appendix F).

Virtually the same caveats discussed above apply to this issue. While we may be more certain about the cost of a brassboard unit, we have no basis for judging what features may ultimately be required by the user, what elements will be part of the Support System, what elements will require interface with the portal unit, or whether the user will want to field a stand-alone system, not interfaced and integrated with the AECS. As a result, our best estimate of $3,835 per portal cost should also be considered rough order of magnitude, based on information known today.

5.3.6 Estimate of Installation Costs (Appendix G).

Notwithstanding the caveats above and in Appendix G, the installation costs are estimated at $500 per portal, not including any related facility renovations or extensive LAN links.

5.3.7 Design Concept (Appendix H).

The design concept of Appendix H is understandably very general at this point. It stresses maximum utilization of commercially available, off the shelf components, interchangeability, modularity, and standard human engineering practices. For a graphic representation of the design concept, see Figures B-1, B-2, and B-3 of Appendix B.

5.3.8 Strawman Deployment POA&M (Appendix I).

5.3.8.1 <u>Introduction</u>. A deployment POA&M is perhaps premature at this stage of development; however, it may serve to highlight some of the unique issues involved in deployment of a biometric Identifier/Verifier (IV) with the potential of the IriScan system. Because the approved AECS specification includes a card reader port with a standard interface, an iris-based IV could well be deployed in minimal time if its initial deployment is limited to AECS applications. Much of the design and engineering effort necessary to field a complete AECS "system" has been accomplished. Therefore, the addition of a biometric device should have significant savings in time and money under options available to the DoD community.

5.3.8.2 <u>Concept</u>. The attached Gantt chart (POA&M) reflects several ideas that support the foregoing premise.

a. Initial deployment of a biometric device as an add-on to a previously designed and approved system will avoid (initially, at least) resources being consumed in designing an entire "system," including card readers, PIN keypads, IDS, alarm monitors, communications, backup power, etc.

b. Initial deployment of a biometric along with the final stages of AECS deployments in FY 97, 98, and 99 would provide a base of experience or lessons learned during initial AECS deployment. That would allow the biometric to interface and operate with completed systems more smoothly and with less potential for incompatibility.

c. With the much smaller "system" inherent in a biometric add-on, production can exceed that of the larger AECS system, and retrofits (adding the biometric device) can proceed concurrently with the last of the larger system installations. Thus, the POA&M reflects completion of deployment of the biometric device concurrent with the larger project.

d. Concentration of resources and rapid transition to Full-Scale Engineering Development could obviate the need for an extended Advanced Development phase.

5.3.8.3 Caveats, Assumptions, Options.

a. The deployment POA&M is based on IriScan meeting design goals and milestones.

b. To meet the ambitious schedule postulated, timely decisions and adequate resources will have to be applied to the project.

c. For non-AECS (or stand-alone) systems, additional engineering and design may be required as a second or adjunct project to enable the biometric devices to be used in conjunction with non-standard systems. Where installations have no requirement for a complete AECS, but need biometrics, support systems and ancillary systems may have to be developed to support biometrics deployment.

d. As costs of biometric production decrease, economies of scale may be such that biometric units at Levels II and I become economically feasible.

e. It is conceivable that the increased security afforded by the IriScan biometric technology could result in reduction or elimination of the redundant security measures (PINS and cards) inherent in the Level III and Level II concept of operation.

5.3.8.4. Elements.

a. The start milestone is only fixed for the purpose of Gantt chart construction. In reality, it is flexible, and can occur either earlier or later than shown.

b. The 12 month Brassboard Development task is based on the POA&M submitted as part of the IriScan proposal. Significantly greater detail is available as part of that document.

c. The time necessary to transition to 6.4 development could be reduced with advanced planning and special emphasis. It has been postulated at approximately one month, given the time frame in which it is expected to occur.

d. Full-Scale Engineering Development (FSED) was projected at 18 months, although one would have to characterize that as a "soft" projection, because it is over one year away and a brassboard decision has not yet been made. One option to speed the overall project is to include a pre-procurement producibility test as part of this task/phase. This would provide units which meet all specifications and can be used in the initial deployment as the more formal procurement phase (P-3080 money) is getting underway.

e. Finally, deployment can proceed as described above with initial biometric deployment meshing with the last of the AECS deployment while simultaneously retrofitting (adding biometric units) to deployed AECS systems. The Gantt chart

(POA&M) could be misinterpreted in that it shows a deployment phase of 34 months. This phase was arbitrarily extended only to reflect the concept that the deployment of a biometric IV should not precede, but should be concurrent with the final stages of initial AECS deployment.

SECTION 6

REFERENCES

1. Barron, Watson; *Computer Resource Management Technology Program (PE 64740F), Task No. 9 - Advanced User Authentication*, PB88-183066; Electronic Systems Division, Hanscom AFB, MA; March 1988; Unclassified.

2. Bright; *Examining The Reliability of A Hand Geometry Identification Verification Device For Use In Access Control*, Thesis, AD-A181 467; Naval Post Graduate School; March 1987; Unclassified.

3. Castain, Payne, Solheim; *Back Propagation Neural Networks for Facial Verification*, LA-12353-MS; Los Alamos National Laboratory; October 1992; Unclassified.

4. Coley; *User Authentication: A State-Of-The-Art Review*, Thesis, AD-A245 612; Naval Post Graduate School; September 1991; Unclassified.

5. Daugman; *High Confidence Personal Identification By Rapid Video Analysis of Iris Texture*; Presentation Paper; International Carnahan Conference on Security Technology Proceedings; October 1992; Unclassified.

6. George; *Electronic Imaging, Final Briefing Report*, AD-A244 319; Institute of Optics, University of Rochester; November 1991; Unclassified.

7. Geshan; *Signature Verification For Access Control*, Thesis, AD-A245 334; Naval Post Graduate School; September 1991; Unclassified.

8. Holmes, Kenna, Murray; *Entry / Exit Control Components For Physical Protection Systems*, SAND92-1339; Sandia National Laboratories; November 1992; Unclassified.

9. Holmes, Maxwell; *Automated Biometric Access Control System For Two-Man-Rule Enforcement*, SAND91-1133; Sandia National Laboratories; August 1991; Unclassified.

10. Holmes, Maxwell, Wright; *A Performance Evaluation of Biometric Identification Devices*, SAND91-0276; Sandia National Laboratories; June 1991; Unclassified.

11. Kuan; *Evaluation Of A Biometric Keystroke Typing Dynamics Computer Security System*, Thesis, AD-A251 788; Naval Post Graduate School; March 1992; Unclassified.

12. Maxwell; *The Status of Personnel Identity Verifiers*; Sandia National Laboratories; July 1985; Unclassified.

13. Maxwell; *Performance Testing Biometric Verifiers*, SAND90-0863; Sandia National Laboratories; March 1990; Unclassified.

14. Miller; *Personal Identification News (PIN) Biometric Technology Handbook*; Warfel & Miller, Inc.; November 1985; Unclassified.

15. Miller; *Personal Identification News (PIN) 1990 Biometric Industry Directory*; Warfel & Miller, Inc.; November 1990; Unclassified.

16. Miller; *Personal Identification News (PIN) The 1994 Advanced Card and Identification Technology Sourcebook*; Warfel & Miller, Inc.; November 1993; Unclassified.

17. Nelson; *Intelligent Facial Recognition Systems, FY93 Final Report*; Nuclear Security Systems Center, Sandia National Laboratories; September 1993; Unclassified.

18. *All About Access Control Systems*, IS42-001-301; Datapro Research Corporation; June 1988; Unclassified.

19. *Computer Voice Recognition: Market Aspects*, Published Search, PB93-866689; National Technical Information Service; September 1993; Unclassified.

20. *System Specification for Advanced Entry Control System (AECS), BISS-SYS-14000*; HQ ESC / AVJM Electronic Security & Communications Center of Excellence, Hanscom AFB, MA; 2 February 1993; Unclassified.

21. *Air Force Space Command Operational Requirements Document (ORD) (USAF ESC 004-88) - I/II/III For Advanced Entry Control System (AECS)*; AFSPACECOM / SPM; 14 April 1993; Unclassified.

1

PERFORMANCE, OPERATIONAL & TECHNICAL REQUIREMENTS MATRIX MA

09-Dec-93
08:34 PM

	SYSTEM REQUIREMENTS	Eye-dentify	Voice Strategies	Alpha Ver-A-Tel	ECCO VoiceKey	ITT SpeakerKey	Ensigma Voice	Hand Geometry	Pal
1	USER:	* *	*	*	*		*	* + *	
2	PERFORMS VERIFICATION	YES	YES	YES	YES	YES	YES	YES	
3	PERFORMS IDENTIFICATION	YES	NO	NO	NO	NO		NO	
4	NO MAN IN LOOP	YES	YES	YES	YES	YES	YES	YES	
5	NO CONTACT	NO	NO	NO	NO	NO	NO	NO	
6	NON-INVASIVE	NO	YES	YES	YES	YES	YES	NO	
7	TYPE I FALSE REJECT < 1 %	YES < 0.4%		NO - 5.1%	NO - 4.3%	YES < 1%		YES - 0.1%	NC
8	TYPE II FALSE ACCEPT < 0.1 %	YES - 0		NO - 2.8%	NO - 0.9%	NO - 5%		NO - 0.1%	NC
9	TYPE I -TYPE II CROSSOVER POINT	1.5%	28 %	6.5%	8.2%	2.2%	16 %	3 %	
10	UNIQUE PHYSICAL CHARACTERISTIC	YES							
11	NO COUNTERFEIT W/O SURGERY	YES						NO	
12	DECISION TIME < 5 SEC	YES	NO	NO	NO	NO		YES	
13	VISUAL/AUDIBLE ALIGNMENT FEEDBACK	YES	NO	NO	NO	NO		YES	
14	VISUAL/AUDIBLE ACCEPT/REJECT	YES	YES	YES	YES	YES		YES	
15	EASILY UNDERSTOOD / USED	GOOD	YES	POOR	POOR	GOOD		GOOD	C
16	STANDALONE DATABASE OF 40,000	NO	NO	NO	225	YES		YES	
17	INTEGRATES W/ CENTRAL DATABASE	YES	YES	YES	NO	YES		YES	
18	INTEGRATES W/ EXISTING MIL SYSTEMS	YES	YES	YES	NO	COULD		YES	
19	ENROLLMENT < 2 MIN	YES	YES			NO - 3+ MIN		YES	
20	OPERATING TEMP 32-150 DEGREES F	NO - 122			-15 - 140	YES		YES	
21	OPERATING HUMIDITY 0-95%	NO - 90			YES	YES		YES	
22	OPERABLE AS EXTERIOR SYSTEM	YES			YES	YES		YES	
23	M T B F GOAL 10 000 HOURS (417 DAYS)					SHOULD		YES	
24	M T T REPAIR < 1 HOUR		YES		YES	YES		YES	
25	SIZE < 24"X24"X12"	YES	YES		YES	YES		YES	
26	WEIGHT < 30 LBS	YES	YES		YES	YES		YES	
27	ONE PORTAL PROD UNIT COST < $5000	YES	YES		YES	YES >5 DOORS		YES	
28	MAINTENANCE COST		LOW	LOW	LOW	LOW		MED	
29	OTHER:	* *	*	*	*		*	* + *	
30	NO ACTIVE INPUT	NO	NO	NO	NO	NO	NO	NO	I
31	USER CONCERNS	LASER-AIDS	CONTACT	CONTACT	CONTACT	CONTACT		CONTACT	CO
32	ACQUIRE & DECISION SPEED	2 SEC	14 SEC	13 SEC	6 SEC	6 SEC		5 SEC	5
33	INDIVIDUAL DATA STORAGE SPACE - BYTES	35	3000		1000	15000		9	
34	INITIAL COST - SMALLEST SYSTEM		20000		2000	25000		2150	
35	STATUS:	IN TROUBLE	MARKET	OUT OF PROD	LIMITED DIST	OTHER MKT	MARKET	MARKET	NOT
36	PROBLEMS:	INVASIVE	BKGD NOISE		SENSITIVITY	ACCURACY		CONTACT	
37		CONTACT	CONTACT		ACCURACY		ACCURACY	ACCURACY	
38		ACCEPTANCE	ACCURACY				BKGD NOISE		
39	QUALIFIED ON CRITICAL CRITERIA :	NO	NO	NO	NO	NO	NO	NO	I
40	DEVELOPMENT POTENTIAL:								

* INCLUDES INFORMATION FROM SANDIA NATIONAL LABORATORIES REPORT

\+ INCLUDES INFORMATION FROM NAVAL POST GRADUATE SCHOOL THESIS

APPENDIX A

PERFORMANCE, OPERATIONAL & TECHNICAL REQUIREMENTS MATRIX

MARKET SYSTEMS

d etry	Palmguard	Stellar Identimat	Identix TouchLock	Trans Sec Ltd Sig Dynamics	Auto-Sig	Xenetex Sig Dynamics	C I C On-Line	Capital Sec Sys Sign/On	Keystroke BioLock	NeuroMetrics Face
*	*	*	* * *	*	*	*	+	+	+	*
S	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
.	NO	NO	NO	NO	NO	NO	NO	NO	NO	YES
S	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
O	NO	NO	NO	NO	NO	NO	NO	NO	NO	YES
O	NO	NO	NO	YES	YES	YES	YES	YES	YES	YES
.1%	NO - 2 %	NO - 1-4 %	NO - 9.4%	NO - 15.1%	NO - 2.1%		NO - 1.4 %	NO - 2.4 %	NO - 4.4 %	
.1%	NO - 2 %	NO - 1-4 %	YES - 0	NO - 5.8%	NO - 0.43%		YES - 0.05 %	NO - 0.9 %	NO - 3.4%	
%		.	5 %			17 %				
	YES		YES	NO	NO	NO	NO	NO	NO	NO
O			NO	NO	NO	NO	NO	NO		
S	YES	NO	YES	NO	NO				NO	NO
S			NO	YES	NO		YES	YES	NO	NO
S			YES		YES		YES	YES	YES	YES
OD	GOOD		FAIR		POOR		YES	YES	GOOD	
S			NO	NO	NO				NO	YES
S			YES		YES	NO	NO		YES	NO
S			YES		YES	NO	NO		NO	NO
S			YES	NO					YES	
S			NO - 32-104						NO	
S			NO -10-90%						NO	
E			YES						NO	
S										
S									YES	
S			YES		YES		YES	YES	YES	
S			65 LBS				YES	YES	YES	
S			YES						YES	
O			NONE ?						LOW	
*	*	*	* * *	*	*	*	+	+	+	*
O	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
ACT	CONTACT	CONTACT	CONTACT	CONTACT	CONTACT	CONTACT	CONTACT	CONTACT	CONTACT	NONE
EC	5 SEC	6 SEC	5 SEC	12 SEC	12 SEC				6 SEC	SLOW
			900	65					250 EST	
0									100	
KET	NOT PROD	OUT OF PROD	MARKET	UNKNOWN	CO GONE	MARKET	MARKET	CO GONE	OTHER MKT	5 YR DEVEL
ACT			CONTACT			CONTACT	CONTACT		NEGOTIATING SALE	ROTATION
RACY			ACCURACY			ACCURACY	ACCURACY			GLASSES
										EXPRESSION
O	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

(1)

PERFORMANCE, OPERATIONAL & TECHNICAL REQUIREMENTS MATRIX

R & D I

09-Dec-93

08:42 PM

	SYSTEM REQUIREMENTS	Sonetech Voice	AUM Systems Voice	LANL Voice	M I T Eigenfaces	Anal Face	Mikos Face	I S N Face	Neilsen/Bel Face
1	USER:			*	*		*		
2	PERFORMS VERIFICATION	YES	YES	YES	YES	YES	YES	YES	YES
3	PERFORMS IDENTIFICATION		YES	NO	YES		YES		YES
4	NO MAN IN LOOP		YES	YES	HELPS		YES		YES
5	NO CONTACT			NO	YES	YES	YES	YES	YES
6	NON-INVASIVE				YES	YES	YES	YES	YES
7	TYPE I FALSE REJECT < 1 %		YES - 1 %	NO - 9.5 %	HIGH				
8	TYPE II FALSE ACCEPT < 0.1 %			NO - 17.7 %	VERY LOW				
9	TYPE I -TYPE II CROSSOVER POINT								
10	UNIQUE PHYSICAL CHARACTERISTIC	NO	NO	NO	NO	NO	NO	NO	NO
11	NO COUNTERFEIT W/O SURGERY				NO	NO	NO	NO	NO
12	DECISION TIME < 5 SEC		YES	NO	YES				
13	VISUAL/AUDIBLE ALIGNMENT FEEDBACK			YES					
14	VISUAL/AUDIBLE ACCEPT/REJECT			YES					
15	EASILY UNDERSTOOD / USED								
16	STANDALONE DATABASE OF 40,000								
17	INTEGRATES W/ CENTRAL DATABASE								
18	INTEGRATES W/ EXISTING MIL SYSTEMS		YES						
19	ENROLLMENT < 2 MIN		YES	NO					
20	OPERATING TEMP 32-150 DEGREES F								
21	OPERATING HUMIDITY 0-95%								
22	OPERABLE AS EXTERIOR SYSTEM								
23	M T B F GOAL 10,000 HOURS (417 DAYS)								
24	M T T REPAIR < 1 HOUR								
25	SIZE < 24"X24"X12"								
26	WEIGHT < 30 LBS								
27	ONE PORTAL PROD UNIT COST < $5000						NOT NOW		
28	MAINTENANCE COST								
29	OTHER:			+	*		*		
30	NO ACTIVE INPUT	NO	NO	NO	YES		YES		YES
31	USER CONCERNS				NONE				
32	ACQUIRE & DECISION SPEED		5 SEC	18 SEC					
33	INDIVIDUAL DATA STORAGE SPACE - BYTES		1000	1000					
34	INITIAL COST - SMALLEST SYSTEM								
35	STATUS:	MID DEV	EARLY DEVEL	UNKNOWN	EARLY DEVEL	EARLY DEV	EARLY DEV	EARLY DEV	SPENT $9 M
36	PROBLEMS:	NA	VULNERABILITY		ROTATION	NA	COST	NA	ROTATION
37			ACCURACY		EXPRESSION	2 CAMERA	ACCURACY		EXPRESSION
38			BKGD NOISE		ACCURACY				ACCURACY
39	QUALIFIED ON CRITICAL CRITERIA :		NO						
40	DEVELOPMENT POTENTIAL:	NA	MODERATE	UNKNOWN	NA	NA	NA	NA	LOW

* INCLUDES INFORMATION FROM SANDIA NATIONAL LABORATORIES REPORT

\+ INCLUDES INFORMATION FROM NAVAL POST GRADUATE SCHOOL THESIS

(2)

R & D PROJECTS

N :e	Neilsen/Bell Face	Sarnoff Face	E-Metrics Face	Physical Optics Face	SD-SCICON Face	LANL Face	U of Illinois Face	T A S C Face	U S C Face	Rutgers Face	IriScan
		*	*	*	*						
S	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
	YES										YES
	YES	YES									YES
S	YES										YES
S	YES	YES	YES	YES	YES	-	YES	YES	YES	YES	YES
											YES
											YES
											0.00076%
)	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	YES
)	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	YES
											YES
											YES
											YES
											YES
											YES
											YES
											YES
											YES
											YES
											YES
											YES
											YES
											YES
											YES
											YES
											YES
											LOW
		*	*	*	*						
	YES	NO									YES
											LIGHT ?
											2 SEC
											500
											3200
DEV	SPENT $9 M	EARLY DEVEL	EARLY DEVEL	EARLY DEVEL	EARLY DEVEL	EARLY DEVEL	EARLY DEVEL	EARLY DEVEL	EARLY DEVEL	EARLY DEVEL	MID-DEVEL
\	ROTATION	OTHER MKT	ROTATION	ROTATION	ROTATION	ROTATION	ROTATION	ROTATION	ROTATION	ROTATION	LIGHTING
	EXPRESSION	ACCURACY	EXPRESSION	EXPRESSION	EXPRESSION	EXPRESSION	EXPRESSION	EXPRESSION	EXPRESSION	EXPRESSION	
	ACCURACY		ACCURACY	ACCURACY	ACCURACY	ACCURACY	ACCURACY	ACCURACY	ACCURACY	ACCURACY	
											YES
\	LOW	LOW	LOW	LOW	LOW	LOW	LONG-TERM	LONG-TERM	LONG-TERM	LONG-TERM	VERY HIGH

ITEM NOTES:

1 ITEMS 2 - 28 ARE SYSTEM REQUIREMENTS ESTABLISHED BY THE USER - DNA & ESC.
2 THIS SYSTEM IS CAPABLE OF VERIFYING THAT A DATA FILE SELECTED BY PIN OR CARD MATCHES CAPTURED BIOMETRIC DATA.
3 THIS SYSTEM IS CAPABLE OF IDENTIFYING AN ENTRANT FROM CAPTURED BIOMETRIC DATA ONLY.
4 ONCE BIOMETRIC DATA IS CAPTURED, THE SYSTEM IS FULLY AUTOMATED (NO HUMAN DECISION INPUT IS REQUIRED) FOR IDENTIFICATION / VERIFICATION.
5 THE DESIRED SYSTEM WILL REQUIRE NO PHYSICAL CONTACT BETWEEN AN ENTRANT AND ANY HARDWARE OR EQUIPMENT PRIOR TO ENTRY AUTHORIZATION.
6 THE DESIRED SYSTEM DOES NOT REQUIRE IMAGES OR FLUIDS FROM INSIDE THE HUMAN BODY, NOR IMPRINTS OF THE EXTERIOR OF THE BODY.
7 THE FALSE REJECTION RATE IS LESS THAN ONE PER HUNDRED.
8 THE FALSE ACCEPTANCE RATE IS LESS THAN ONE PER THOUSAND.
9 THE POINT WHERE FALSE REJECTS EQUAL FALSE ACCEPTS IS BELOW 0.1 % AND IS IDENTIFIED, IF KNOWN.
10 THIS SYSTEM IS BASED UPON MEASUREMENT OF A UNIQUE PHYSICAL, NOT BEHAVIORAL, CHARACTERISTIC.
11 IS IT POSSIBLE TO CREATE A COUNTERFEIT OF THE BIOMETRIC SAMPLE, WITHOUT SURGICAL MODIFICATION OF THE HUMAN PHYSIOGNOMY.
12 THE TIME BETWEEN CAPTURE OF THE BIOMETRIC DATA AND ANNUNCIATION OF THE ACCEPT / REJECT DECISION IS LESS THAN FIVE SECONDS.
13 THE SYSTEM PROVIDES EITHER VISUAL OR AUDIBLE ALLIGNMENT FEEDBACK TO ENHANCE BIOMETRIC DATA CAPTURE.
14 THE SYSTEM PROVIDES EITHER VISUAL OR AUDIBLE ANNUMCIATION OF THE ENTRANCE AUTHORIZATION OR REJECTION DECISION.
15 THE SYSTEM AND THE ENTRANT ACTIONS REQUIRED ARE EASILY UNDERSTOOD AND APPLIED.
16 THE SYSTEM WILL BE ABLE TO COMPARE PRESENTED BIOMETRIC DATA TO A STORED DATABASE OF 40,000 FILES.
17 THE SYSTEM WILL BE ABLE TO INTEGRATE AND OPERATE WITH A SINGLE, CENTRAL DATABASE.
18 THE SYSTEM WILL BE ABLE TO INTEGRATE AND OPERATE WITH EXISTING MILITARY SECURITY AND ACCESS CONTROL SYSTEMS.
19 THE TOTAL TIME REQUIRED FOR COLLECTION OF BIOMETRIC ENROLLMENT DATA (EXCLUSIVE OF ADMINISTRATIVE DATA) IS LESS THAN TWO MINUTES.
20 THE SYSTEM IS CAPABLE OF SUSTAINED OPERATIONS IN TEMPERATURES BETWEEN 32 AND 150 DEGREES F.
21 THE SYSTEM IS CAPABLE OF SUSTAINED OPERATIONS IN HUMIDITY CONDITIONS BETWEEN 0 AND 95 %.
22 THE SYSTEM IS CAPABLE OF SUSTAINED OPERATIONS IN AN EXTERIOR ENVIRONMENT.
23 THE MEAN TIME BETWEEN FAILURE (MTBF) GOAL FOR THE SYSTEM IS 10,000 HOURS.
24 THE MEAN TIME TO REPAIR (MTTR) REQUIRED IS ONE HOUR (AVERAGE TIME TO REPAIR ANY FAILURE IS LESS THAN ONE HOUR).
25 SELF-EXPLANATORY.
26 SELF-EXPLANATORY.
27 IN MARKET PRODUCTION NUMBERS, THE TOTAL COST FOR A SYSTEM TO CONTROL ACCESS AT ONE PORTAL IS LESS THAN $5,000.
28 ESTIMATED PREVENTIVE MAINTENANCE COST FOR THE SYSTEM IS (LOW, MEDIUM, HIGH).
29 OTHER DATA CONCERNING THE SYSTEM WHICH IS CONSIDERED IMPORTANT TO DEVELOPMENT DECISION-MAKING.
30 CAN THE SYSTEM OPERATE WITH NO ACTIVE INPUT FROM THE ENTRANT?
31 ARE THERE ANY FACTORS CONCERNING SYSTEM OPERATION WHICH ARE OF CONCERN TO SYSTEM USERS?
32 WHAT IS THE TIME REQUIRED TO CAPTURE NECESSARY BIOMETRIC DATA AND ANNOUNCE AN AUTHORIZATION DECISION.
33 HOW MANY BYTES ARE REQUIRED TO STORE THE DATA FILE FOR ONE INDIVIDUAL?
34 WHAT IS THE INITIAL COST OF THE SMALLEST (ONE-PORTAL) SYSTEM AVAILABLE?
35 WHAT IS THE CURRENT STATUS OF THE PRODUCT, COMPANY, OR DEVELOPMENT PROJECT?
36-3 ARE THERE ANY KNOWN OR POTENTIAL PROBLEMS INVOLVING THE UTILIZATION OF THE SYSTEM?
39 DOES THE SYSTEM MEET ALL CRITICAL CRITERIA? (CAN PERFORM IDENTITY VERIFICATION WITH NO HUMAN IN THE OPERATION / DECISION LOOP,

NO PHYSICAL CONTACT WITH THE ENTRANT
NO INVASIVE BIOMETRIC DATA CAPTURE
FALSE REJECT RATE LESS THAN 1.0 %
FALSE ACCEPT RATE LESS THAN 0.1 %
TYPE I - TYPE II ERROR CROSSOVER POINT LOWER THAN 0.1 %
BASED UPON A UNIQUE PHYSICAL CHARACTERISTIC.

40 WHAT IS THE ESTIMATED DEVELOPMENT POTENTIAL OF THIS SYSTEM?

SYSTEMS:

RETINA SCAN	EYEDENTIFY INC., 11931 INDUSTRIPLEX BLVD, SUITE 300, BATON ROUGE, LA 70809, (800) 593-5353, FAX (504) 752-5798
VOICE	VOICE STRATEGIES, 4555 CORPORATE DRIVE, SUITE 304, TROY, MI 48098, (313) 641-8600, FAX (313) 641-8590
VOICE- VER-A-TEL	ALPHA MICROSYSTEMS, 3501 SUNFLOWER, SANTA ANA, CA 92704, (714) 957-8500, (GARY NELSON), OUT OF PRODUCTION.
VOICE-KEY	INTERNATIONAL ELECTRONICS, INC., 32 WEXFORD STREET, PO BOX 584, NEEDHAM HEIGHTS, MA 02194, 1-800-343-9502, (SCOTT RACINE)
VOICE-SPEAKER-KEY	ITT AEROSPACE / COMMUNICATIONS DIVISION, 1919 WEST COOK ROAD, PO BOX 3700, FT. WAYNE, IN 46801, (219) 487-6000, FAX (219) 487-6126
VOICE	ENSIGMA
HAND GEOMETRY	RECOGNITION SYSTEMS, INC., 1589 PROVINCETOWN DRIVE, SAN JOSE, CA 95129, (408) 364-6960 FAX (408) 370-3679, (BILL WILSON)
PALMPRINT	PALMGUARD
FINGER LENGTH	STELLAR IDENTIMAT,
FINGERPRINT	IDENTIX, INC., 510 N. PASTORIA AVE, SUNNYVALE, CA 94086, (408) 739-2000, FAX (408) 739-3308, (DAVID JACKSON)
SIGNATURE DYNAMICS	TRANSACTION SECURITY, LTD,
SIGNATURE AUTO-SIG	CAPITAL SECURITY SYSTEMS, INC., 9050 RED BRANCH ROAD, COLUMBIA, MD 21045, (410) 730-8250, DISCONNECTED.
SIGNATURE DYNAMICS	XENETEX
SIGNATURE DYNAMICS	COMMUNICATION INTELLIGENCE CORP.,
SIGNATURE DYNAMICS	CAPITAL SECURITY SYSTEMS, INC.. 9050 RED BRANCH ROAD, COLUMBIA, MD 21045, (410) 730-8250, DISCONNECTED.
KEYSTROKE	PHOENIX SOFTWARE INTERNATIONAL, 5933 W CENTURY BLVD, SUITE 1200, LOS ANGELES, CA 90045, 1-800-622-9292, (KEVIN KEYES)
FACE RECOGNITION	NEUROMETRIC VISION SYSTEMS, INC., 3720 PARK CENTRAL BLVD NORTH, POMPANO BEACH, FL 33064, (305) 972-0559, FAX (305)972-0197 (BILL GEE)
IRIS SCAN	IRISCAN, INC., 133Q GAITHER DRIVE. MT. LAUREL, NJ 08054, (609) 234-7977, FAX (609) 234-4768
VOICE TEXT IND	SONETECH, 47 CONSTITUTION DRIVE, BEDFORD, NH 03110, (603) 472-2055, FAX (603) 472-8738 (HARVEY WOODSUM)
VOICE TEXT IND	A U M SYSTEMS,P.O.BOX 960, NEW BRUNSWICK, NJ, (908) 220-1100, FAX (908) 220-1621, (PRACASH SHUKLA)
VOICE	LOS ALAMOS NATIONAL LABORATORY, LOS ALAMOS. NM 87545, (505)667-3283, FAX (505) 665-4109 (RALPH H. CASTAIN / WINDELL FORD)
FACE RECOGNITION	M I T MEDIA LAB, 20 AMES STREET, CAMBRIDGE, MA 02139, (617) 253-0648, FAX (617) 253-8874 (PROF ALEX PENTLAND)
FACE RECOG 90 DEG	ARIAL TECHNICAL SERVICES, CA, (714) 573-2818, FAX (714) 573-2817 (DAVID W. HAMILTON, PRES)
FACE THERMOGRAPHY	MIKOS LTD, CIT TOWER, SUITE 300, 2214 ROCK HILL ROAD, HERNDON, VA 22070, (703) 478-7260, FAX (703) 478-7254 (FRANCINE J. PROKOSKI, PRES)
FACIAL RECOGNITION	INFORMATION SYSTEMS NETWORK, INC., 10411 MOTOR CITY DRIVE, BETHESDA, MD, (301) 469-0400, (DR NENNINGER)
FACIAL RECOGNITION	A C NIELSEN, 2675 N SANDERS RD, NORTHBROOK, IL 60062, (708) 498-6300 x7290 (ED SCHILLMOELLER)
FACIAL RECOGNITION	DAVID SARNOFF RESEARCH CENTER
FACIAL RECOGNITION	E-METRICS (GEN DYNAMICS SUBSIDIARY)
FACIAL RECOGNITION	PHYSICAL OPTICS
FACIAL RECOGNITION	SD-SCICON
FACIAL RECOGNITION	LOS ALAMOS NATIONAL LABORATORY, LOS ALAMOS, NM 87545, (505)667-3283, FAX (505) 665-4109 (RALPH H. CASTAIN)
FACIAL RECOGNITION	UNIVERSITY OF ILLINOIS, 809 SOUTH MARSHFIELD STREET, CHICAGO, IL 60612.
FACIAL RECOGNITION	THE ANALYTIC SCIENCES CORP., READING, MA 01867.
FACIAL RECOGNITION	UNIVERSITY OF SOUTHERN CALIFORNIA, UNIVERSITY PARK, LOS ANGELES, CA 90089.
FACIAL RECOGNITION	RUTGERS, THE STATE UNIVERSITY, CAIP, P.O.BOX1089, PISCATAWAY, NJ 08855-1089.

APPENDIX B

SUPPORT SYSTEMS REQUIREMENTS

FOR A DOD IRIS RECOGNITION SYSTEM

B.1 INTRODUCTION.

B.1.1 Purpose.

This document is intended to prescribe the requirements for the "support" portion of an identification/verification (IV) system. The support portion of the system is that series of functions not directly related to acquiring the image of an eye, encoding the image, comparing it to a stored data base, making a determination of authentic or imposter, and providing some output about that determination. Those functions, known as the Technical System Functions (TSF) are essentially the heart or "core" of the IV (IriScan) process and have been defined in Technical System Requirements.

By contrast, there are many functions outside that determination process which must be completed in order to provide a fully capable IV "system." These are not new or innovative functions, but ones which are fundamental to any and all entry or access control systems. This document is intended as a guide for either development or procurement of hardware and software necessary to perform the many functions ancillary but necessary to implementing the identification/verification decision.

B.1.2 Scope.

B.1.2.1 General. Because of the infinite variety of potential installations of an IV system, no two configurations will be precisely the same. There are, however, a finite number of major generic configurations which can result from a user's requirements. These become more apparent when considering what the user needs, what exists now, and what resources are available. Following are some major configurations which seem reasonable.

a. Single Portal (Master Unit). A single IV unit, self contained. Enrollment and identification occur at same portal. Unit powers a single electric door strike.

b. Multiple Portals (Slave Units). More than one IV unit (Up to 5 slaves controlled by 1 Master). Enrollment can occur at a single, "master" unit. "Slave" units control electric strikes.

c. Complete System. Numerous portals (More than the 6 described above). Centralized enrollment, database, and system control. This system configuration provides a complete, "from scratch" system where nothing has existed before. Provides to user <u>all</u> entry / access control functions.

d. Biometric Input Device Only. Unit identifies or verifies identity of entrant and provides signal to existing port on processor, control unit, or card-reader.

e. Integrated With Existing System. Multiple portals. Replaces card readers. Centralized enrollment and data input to existing CPU.

B.1.2.2 <u>Scope of this Document</u>. Having considered the numerous configurations possible for IV units and systems, and having reduced those to the manageable number outlined in the foregoing paragraph, it is possible to analyze all the functions of these configurations and conclude that IV units will perform like functions for multiple configurations. We are thus able to reduce the various types of units (and their requirements) to the minimum number that accommodate all the anticipated configurations. In some cases a unit selected for a particular configuration will come off the production line able to perform more functions than required or desired by the custome . The units should be designed so that these extraneous functions can be easily disabled manually, through factory adjustments, or through field selectable (operator) actions. The scope of this document will therefore address the functions and requirements of only a "Master" unit, a "Slave" unit, and a complete IV "system." These three configurations are detailed in Figures B-1, B-2, and B-3.

B.1.2.3 The Support Subsystem. An IV system (single or multiple units) is comprised of hardware and a computer program. A computer program is a series of instructions or statements, in a form acceptable to the computer, designed to cause the computer to execute an operation or series of operations. The software subsystem is an organization of lower-level elements (modules of code), excluding all other classes of instructions such as key strokes, card readers, and alarms. The purpose of the IV Support System Software subsystem is to provide all functions of an automated entry/access control system, except the identification or verification of identity. The support computer program interfaces with the Technical System Software (TSS) to permit enrollment and verification of enrollment. It also interfaces with the TSS to act on the identification or verification determinations of that portion of the system. The computer program interfaces with various input and output devices (CRT, printer, enrollment station, card readers, alarm outputs, etc.) to provide for alarm and system monitoring and control.

B.1.3 Functional Summary.

Following is a summary, by unit configuration, of the functions that a support system should be capable of performing.

B.1.3.1 IV Master Unit (IMU).

a. Monitor Door Contact Switch.

b. Shunt Alarm on Valid Entry.

c. Activate Strike.

d. Generate Alarms.

(1) Access Denied Alarms:

- Unidentified Person. Failure of the TSS module to match a presented iriscode with a database iriscode.
- Invalid Time. Individual attempting entry is enrolled in system, but is not authorized access through that portal in the current time period.
- Invalid Portal. Individual attempting entry is enrolled in system, but is not authorized access to that portal.
- No exit. In a system where there are both ingress and egress IV Slave Units (ISUs) (Personnel Tracking), the IMU must detect when an individual has entered a portal, but exited without using the exit ISU inside the space.

(2) Portal Open Alarms. (See para. B.3.1.1, below)

- Portal open too long.
- Release Emergency.
- Intrusion.

(3) Unauthorized Function Attempt. An attempt by in individual to manipulate the IMU control panel in such a way as to enroll, dis-enroll, or manually shunt the system, when that individual is not authorized to perform those functions, or when two authorized individuals are not present, depending on how the system is programmed.

(4) Duress Alarm. Manual activation of the covert device on the control panel indicating that an operator or entrant is under duress.

(5) Trouble alarm. A condition reported by the IMU's sub-components when the component fails a self-test.

(6) Line Supervision Alarm. A condition recognized by the communications module when it senses tampering or loses contact with a Slave Unit (ISU).

(7) Tamper Alarm. Removal or attempted removal of the cover of the IMU.

e. Enroll/Dis-Enroll.

(1) Supervisory privilege, or two-person control.

(2) Controls for enrolling/dis-enrolling.

(3) Establish access level. (As a minimum, who can enroll/dis-enroll.)

(4) Visual/audible indication of good/bad enrollment/dis-enrollment.

f. Control of "Slave" Units: (up to 5).

(1) Control of communications protocol.

(2) Provide insert/delete file instructions to slaves.

(3) Download file data to slave units.

g. Generate Reports.

h. Provide Input for Testing/Troubleshooting.

B.1.3.2 <u>IV Slave Units (ISU)</u>.

a. Monitor Door Contact Switch.

b. Shunt Alarm on Valid Entry.

c. Activate Strike.

d. Recognize, Distinguish, and Report (to the Master) the Alarms Listed Above.

e. Accept and Act on File Insertion/Deletion Instructions.

f. Provide Input for Testing/Troubleshooting.

g. Generate and Transmit Reports to Master.

B.1.3.3 Complete IV System.

a. Functions to be Performed in the Portal Segment of the System.

(1) Monitor door contact switch.

(2) Shunt alarm on valid entry.

(3) Activate door strike on valid entry.

(4) Generate and report alarms.

Access Denied Alarms:
Unidentified Person.
Invalid Time.
Invalid Portal.

No exit.

Portal Open Alarms.

Portal open too long.

Release Emergency.

Intrusion.

Unauthorized function attempt.

Duress alarm.

Trouble alarm.

Line Supervision Alarm.

Tamper alarm.

(5) Accept and act on file creation/deletion instructions.

(6) Generate status reports when queried.

(7) Facilitate testing and diagnostics.

b. Functions to be Performed in the Monitor/Control Segment of the System.

(1) Provide visual and audible alerts to operator. Distinguish between types of alarms and structure alerts to convey visual and audible clues as to the type and priority of such alarms.

(2) Provide visual indications of system status, including remote units. As a minimum, provide the following:

Secure.

Alarm & type.

Shunt.

(3) Provide for manual shunt control.

(4) Maintain central database, including Personal Identification Records on each enrollee in the system.

(5) Provide for enrollment.

(6) Store data and provide for retrieval and report generation in the following minimum categories:

Enrollments.
Entrances & exits by portal and time.
Alarms.
Trouble reports.
Maintenance actions.
Site adaptation changes.
List of persons inside each area.

(7) Provide for active system status verification (polling).

c. Functions to be Performed by the Communications Segment of the System.

(1) External communications.

- Communicate all transactions (alarms, entrances, exits, maintenance actions, etc) from the Portal Segment to the Monitor/Control segment.
- Communicate instructions and polling inquiries from the Monitor/Control Segment to the Portal Segment.
- Communicate enrollment transactions (including iris codes) from the enrollment terminal to the CPU database.
- Monitor and report line failures.
- Encrypt/decrypt data where necessary.

(2) Internal communications.

- Communicate alarm and status change information from buffer to database and audible/visual indicators.
- Communicate instructions and inquiries from the keyboard and other input devices to the CPU.
- Communicate report data from buffer to output devices.

B.1.4 Assumptions and Constraints.

a. This is a dynamic document rather than a final, finished product. It is intended to be revised and updated as the requirements analysis progresses and matures.

b. This functional requirements document is being written to facilitate the IV development process rather than as a stand-alone deliverable. It is therefore not constructed and formatted in accordance with MILSPECs or MILSTDs.

c. This document was initially created not by engineers, but by systems analysts whose primary perspective is that of the user(s) of the system. Thus the focus is on a functional requirement analysis as opposed to any preconceived hardware/software design scheme.

B.2 DOCUMENTS.

The following publications relate to this document:

a. *Technical System Requirements for a DoD Iris Recognition System*, IriScan Incorporated, Kuhla, Cletus B., 1993.

b. *The Software Development Project*, Pederson, Sam M. and Phillip, Bruce, John Wiley & Sons, New York, NY, 1982.

c. *Operational Requirements Document 004-88*, United States Air Force, 1988

d. *System Specification for Advanced Entry Control System (AECS) (DRAFT)*, BISS-SYS-14000, HQ Electronic System Division/AVJ, May 1991

B.3 REQUIREMENTS.

B.3.1 IV Master Unit (IMU)

B.3.1.1 Monitor Door Contact Switch. The door contact switch (normally open/normally closed) will be hardwired to the IMU. By sensing voltage fluctuations, the IMU must recognize door secure, door open, trouble, and line failure. Additionally, the IMU must recognize if the Door Open alarm is accompanied by activation of the emergency release, or if the door has been open beyond the preset allowable interval. The IMU will initiate a priority interrupt message to the Monitor/Control Segment of the system. The message must identify the condition as Portal Open--Too long, Portal Open--Emergency Release, Portal Open--Intrusion, Trouble, or Line Supervision.

B.3.1.2 Shunt Portal Open Alarm. The IMU will be capable of recognizing that a valid identification has been made, noting that door opening has been authorized, and shunting the Portal Open alarm for a preset interval to prevent erroneous upchannel reporting. Additionally, the IMU will have the capability to accept shunt commands from the Monitor/Control Segment, or from manual activation of the controls on the IMU control panel.

B.3.1.3 Activate Strike. The IMU will be capable of sensing a signal from the Support System Software (SSS) module authorizing the portal to be opened. The IMU will be capable of initiating a signal to the electric strike mechanism to close a relay and energize the strike release mechanism for a preset, programmable period of time to allow entry.

B.3.1.4 Generate Alarms. The IMU will be capable of recognizing a variety of alarms, formatting reports, and forwarding the report messages to the Monitor/Control Segment of the system. These include the following:

a. Access Denied Alarms:

- Unidentified Person. Failure of the TSS module to match a presented iriscode with a database iriscode.
- Invalid Time. Individual attempting entry is enrolled in system, but is not authorized access through that portal in the current time period.
- Invalid Portal. Individual attempting entry is enrolled in system, but is not authorized access to that portal.
- No exit. (In a system where there are both ingress and egress IV Slave Units (ISUs) (personnel tracking), the IMU must detect when an individual has entered a portal, but exited without using the exit ISU inside the space.

b. Portal Open Alarms. (See para. B.3.1.1 above)

Portal open too long.
Release Emergency.
Intrusion.

c. Unauthorized Function Attempt. An attempt by in individual to manipulate the IMU control panel in such a way as to enroll, dis-enroll, or manually shunt the system when that individual is not authorized to perform those functions, or when two authorized individuals are not present, depending on how the system is programmed.

d. Duress Alarm. Manual activation of the covert device on the control panel indicating that an operator or entrant is under duress.

e. Trouble Alarm. A condition reported by the IMUs sub-components when the component fails a self-test.

f. Line Supervision Alarm. A condition recognized by the communications module when it senses tampering or loses contact with a Slave unit (ISU).

g. Tamper alarm. Removal or attempted removal of the cover of the IMU.

B.3.1.5 Enrollment/Dis-Enrollment. The IMU will incorporate and be integrated with the SSS module to enable the enrollment or dis-enrollment of subjects in the system. This capability includes sufficient and adequate controls/devices on the exterior of the IMU to accomplish such functions including visual/audible indication of successful or unsuccessful enrollment/dis-enrollment. The control panel will have the capability to establish access levels for enrollees, including as a minimum, who is authorized to enroll/dis-enroll. In addition, the IMU will be capable of recognizing that the person attempting the function is authorized to perform the action, or that the system has been programmed for two-person control and that two authorized persons are present.

B.3.1.6 Control of "Slave" Units (up to 5). The IMU will have the capability of controlling communications protocol among 5 slave units reporting to it. It will be capable of downloading file data to slave units, including insert/delete file instructions for incorporation into the slave's respective databases, following a valid enrollment or dis-enrollment at the IMU.

B.3.1.7 Report Generation. The IMU will be capable of reporting information to the Monitor/Control Segment in several modes:

a. Priority interrupt alarm reports.

b. Routine reports of slave and IMU status.

c. Historical transaction reports.

d. Ad hoc reports requested by the Monitor/Control Segment.

B.3.1.8 Database Storage. The IMU will have the capability to store up to 4,000 enrollees (8,000) iriscodes, as well as sufficient storage to store programming instructions, 24 hours of historical transaction data, and other system operating requirements.

B.3.1.9 Input for Testing/Troubleshooting. The IMU will have a functional test jack and internal circuitry to allow a technician to perform diagnostic and programming functions from that jack to all of the IMUs internal modules.

B.3.1.10 Apply Personnel Tracking Logic. In those installations where the system or customer requirements dictate egress as well ingress ISUs, the IMU will have the capability to discern 1) that the entrant has previously been granted entry, and 2) such entry event(s) were followed by an exit. If the entrant has been granted access previously without a corresponding exit, the IMU will deny entry and initiate an Access Denied - No Exit alarm.

B.3.2. IV Slave Units (ISU).

B.3.2.1 Monitor Door Contact Switch. The door contact switch (normally open/normally closed) will be hardwired to the ISU. By sensing voltage fluctuations, the ISU must recognize door secure, door open, trouble, and line failure. The Door Open alarm will be registered under two conditions: physical breach of the door, or the door remaining open beyond a pre-set interval after a valid entry. The ISU will initiate a priority interrupt message to the Monitor/Control Segment of the system; through the IMU in the multi-portal configuration, and through the Remote Control Unit (RCU) in the complete IriScan system.

B.3.2.2 Shunt Portal Open Alarm. The ISU will be capable of recognizing that a valid identification has been made, noting that door opening has been authorized, and shunting the Portal Open alarm for a preset interval to prevent erroneous upchannel reporting. Additionally, the ISU will have the capability to accept shunt commands from the Monitor/Control Segment (IMU or RCU, depending on the system configuration).

B.3.2.3 Activate Strike. The ISU will be capable of sensing a signal from the SSS module to authorize the portal to be opened. The ISU will be capable of initiating a signal to the electric strike mechanism to close a relay and energize the strike release mechanism for a preset, programmable period of time to allow entry.

B.3.2.4 Generate Alarms. The ISU will be capable of recognizing a variety of alarms, formatting reports, and forwarding the report messages to the Monitor/Control Segment of the system. These include the following:

a. Access Denied Alarms.

   Unidentified Person.
   Invalid Time.
   Invalid Portal.
   No exit.

b. Portal Open Alarms.

   Portal Open Too Long.
   Emergency Release.
   Intrusion.

c. Duress alarm.

d. Trouble alarm.

c. Line Supervision Alarm.

d. Tamper alarm.

B.3.2.5 Database Storage. The ISU will have the capability to store up to 4000 enrollees (8000 iriscodes).

B.3.2.6 Accept and Act on File Creation/Deletion Instructions. The ISU will be capable of responding to instructions from the IMU, RCU, and CPU directing the creation or deletion of iriscodes and data files.

B.3.2.7 Input for Testing/Troubleshooting. The ISU will have a functional test jack and internal circuitry to allow a technician to perform diagnostic and programming functions from that jack to all of the ISUs internal modules.

B.3.2.8 Generate and Transmit Reports to Master. The ISU will be capable of reporting information to the Monitor/Control Segment in several modes:

a. Priority interrupt alarm reports.

b. Routine status reports when polled.

c. Ad hoc reports requested by the Monitor/Control Segment.

B.3.2.9 Search Additional Databases for Iriscodes. The ISU will be capable of requesting a comparison of iriscodes when its own database reveals no match for an entrant. This could include other slave units, IMU's, or RCU's. The ISU will not initiate an Unidentified Person alarm until negative responses are received from all addressees of the comparison request.

B.3.3 Complete IV System.

B.3.3.1 Functions to be Performed in the Portal Segment of the System.

NOTE 1: In this configuration, the IV Master Unit would not normally be utilized. It is possible that there may be a small portion of a system, or a remote enclave best served by an IMU; however, the enroll/dis-enroll function might well be disabled to preserve the single, centralized enrollment activity in the Monitor/Control Segment. The slave units, one for each portal, report to an RCU. This RCU is more robust than an IMU, can handle up to 16 IV Slave Units, has an expanded database (10,000 files), and does not have the IMU enrollment/dis-enrollment capability.

NOTE 2: All of the portal functions have been previously discussed in par B.3.2 as functions of the IV Slave Unit, so will be listed, but not detailed here.

a. Monitor door contact switch.

b. Shunt alarm on valid entry.

c. Activate door strike on valid entry.

d. Generate and report alarms.

Access Denied Alarms:
- Unidentified Person.
- Invalid Time.
- Invalid Portal.
- No exit.

Portal Open Alarms.
- Portal Open Too Long.
- Emergency Release.
- Intrusion.

Duress Alarm.

Trouble Alarm.

Line Supervision Alarm.

Tamper Alarm.

d. Database storage.

e. Accept and act on file creation/deletion instructions.

f. Facilitate testing and diagnostics.

g. Generate and transmit reports.

h. Search additional databases for iriscodes.

B.3.3.2 Functions to be Performed by the Communications Segment of the System.

a. The Communications Segment will provide adequate and secure communication of all data between all parts and functions of the complete IV system using high capacity digital communications equipment conforming to EIA-RS-232, EIA-RS-422, or EIA-RS-485 specifications.

b. Communicate all transactions (alarms, entrances, exits, maintenance actions, etc), priority interrupts, and routine responses to polling inquiries from the Portal Segment to the RCU portion of the Monitor/Control Segment and from the RCU to the CPU.

c. Communicate instructions, database updates, and polling inquiries from the Monitor/Control Segment to the Portal Segment.

d. Communicate enrollment transactions (including iriscodes) from the enrollment terminal to the CPU database.

e. Monitor the Communications Segment by providing line supervision checks at least once each second, and report line failure alarms when any portion of the Communications Segment fails.

f. Interface with standard NSA/DoD or commercially available cryptography equipment without degradation of data rate to enable communications to be encrypted and decrypted data where necessary. The interface will be such that the system operates equally well with or without the equipment present and will transition to the non-encrypted mode seamlessly upon failure of the cryptography equipment.

g. Use standard protocols.

h. Provide an interface to the IriScan system equipment which is independent of the transmission mode.

i. The maximum data rate capacity when operating with the operational application computer programs will be 200% of the data rate required by the worst operational situation, assuming the maximum generic configuration (256 portals).

B.3.3.3 Functions to be Performed in the Monitor/Control Segment of the System.

a. Alerts. Provide visual and audible alerts to operator. The system will be able to distinguish between types of alarms, and will structure the audible and visual alerts to inform the operator of the type and priority of such alarms.

b. Display Requirements.

(1) General.

(a) Color coding.

- FLASHING RED shall be used to annunciate all unacknowledged alarms.
- STEADY RED shall be used to alert the operator to an acknowledged alarm.
- YELLOW shall be used to advise the operator that a portal alarm has been shunted.
- GREEN shall be used to indicate that a portal is secure.
- FLASHING of any color shall indicate that the status of the portal has changed, and the change has not been acknowledged.

(b) A cursor bar of the above colors shall be overlaid on the information line with the alpha-numerics supplying the information in a contrasting color.

(2) Status Display.

(a) Provide visual indications of system status, including remote units. As a minimum, provide the following:

- PORTAL NUMBER: (Always set at #1 in Single Portal Configuration.)
- STATUS: Secure.
  - Alarm.
    - Access Denied.
      - Unidentified Person.
      - Unauthorized Time.
      - Unauthorized Portal.
      - No Exit.
    - Portal Open.
      - Portal Open Too Long.

Emergency Release.

Intrusion.

Unauthorized Function Attempt.

Duress.

Trouble (and location/module).

Line Supervision (and segment).

Tamper.

Site power failure.

Low battery in UPS.

(b) For the alarms listed above, provide the following data on a single line:

Alarm priority.

Portal number.

Type of alarm.

Time of alarm.

Auxiliary information.

(c) For any non-alarm status change, provide the following data on a single line:

Portal number (if applicable).

Previous status/new status.

Checklist reference.

(3) Menu data.

(4) Checklist window to provide sequential operator actions or individual prompts in response to an operator-initiated procedure.

c. Printer. The system will provide a software-controlled printer which will automatically print hardcopy reports of each status change, responses thereto, and operator-initiated actions. The printer program should also have the capability to print pre-formatted reports or operator-formatted reports at the operator's request.

d. Keyboard. The system will provide an alphanumeric keyboard with function keys as a primary input device for an authorized system operator.

e. Enrollment. The system shall provide an enrollment function remote from the CPU and system operator. It shall consist of a terminal (CRT and keyboard), interfaced with a TSS module. It will be capable of enrolling individuals into the database, creating files with access levels, transmitting that data to the appropriate repository, soliciting reports about the system status relative to the database and enrollment function, and dis-enrolling or extracting files from the system.

f. Manual Shunt. Provide for manual shunt control. The Monitor/Control Segment will provide the capability for an authorized system operator to initiate a command to a selected portal to shunt (temporarily disable the reporting of) Portal Open alarms.

g. Database. The system will provide for a database, including Personal Identification Records on each enrollee in the system. Each portal will have the capacity for 4,000 enrollees, each RCU 10,000, and the central system database a capacity for 40,000 enrollees. System software will provide for a portal search of its own database, that of the IMU and sister ISUs, RCUs and the central database before registering an Unidentified Person alarm. The software will automatically download file information to the requesting portal if a valid identification is made in other than the primary database.

h. Report Generation. Store data and provide for retrieval and report generation in the following minimum categories:

Enrollments.

Entrances & exits by portal.

Alarms.

Trouble reports.

Maintenance actions.

Site adaptation changes.

List of persons inside each area where client has specified both ingress and egress ISUs at each portal.

i. Polling. Provide for active system status verification (polling).

j. Remote Control Units (RCUs). Intermediate processing units will be provided where more than six (6) portals (three portals where ingress and egress ISUs are specified) must be protected These units have the following functional requirements:

(1) The RCUs will have the physical and functional capability to interface with and control 16 ISUs.

(2) An RCU will have the capability to pass all data to and from the portals to and from other elements of the Monitor/Control Segment.

(3) An RCU will have the capacity to store 10,000 irisfiles and provide to ISUs who's initial search of their own database did not result in a valid identification.

(4) An RCU will have a polling program capable of polling all assigned ISU's and reporting a status change when polled by the main system CPU.

(5) The RCU will be capable of generating alarms as follows:

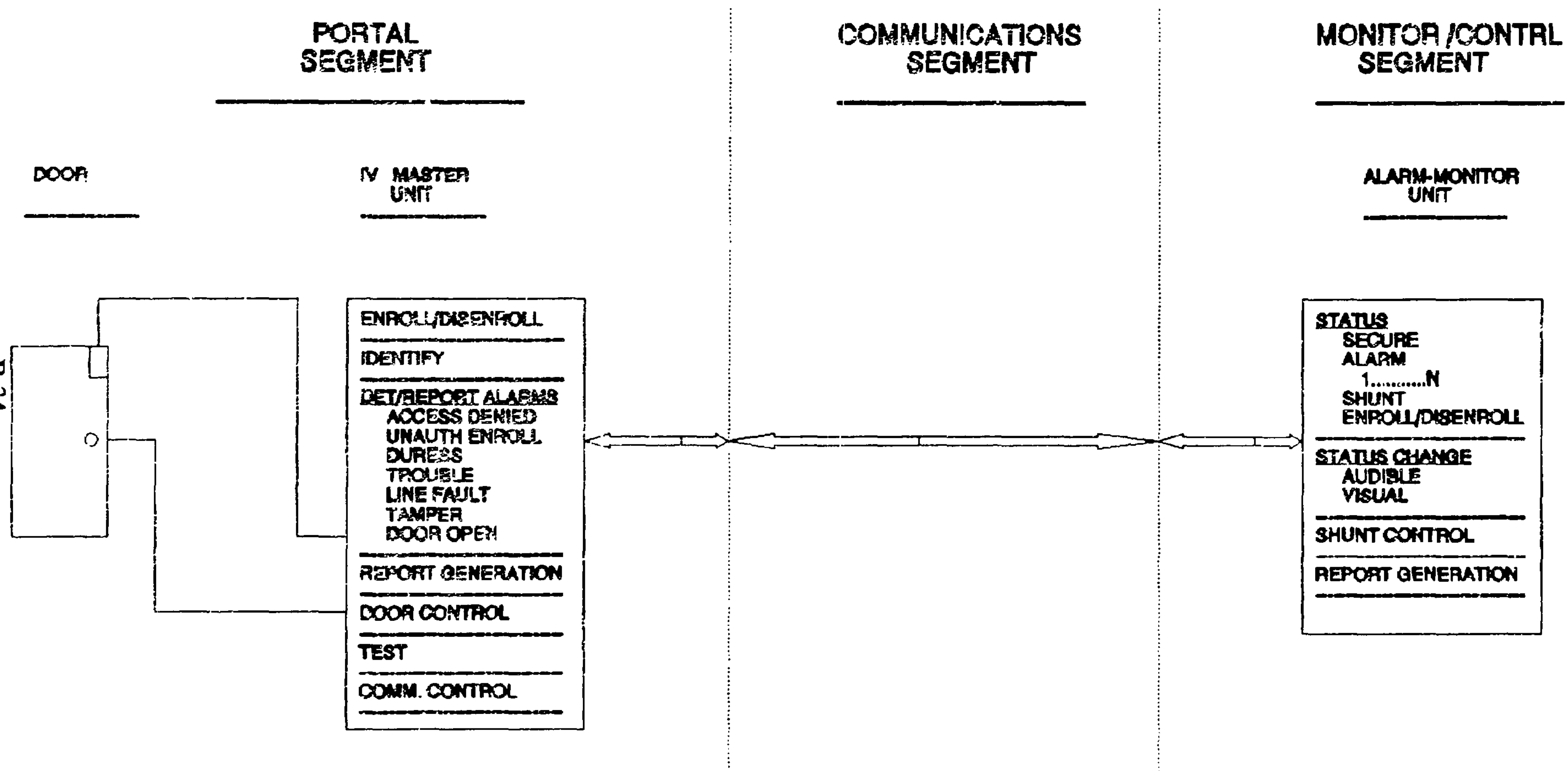
- Trouble (as the result of failure of an internal self-check program).

- Line Supervision (as a result of indications of line tampering or loss of contact with an assigned ISU).

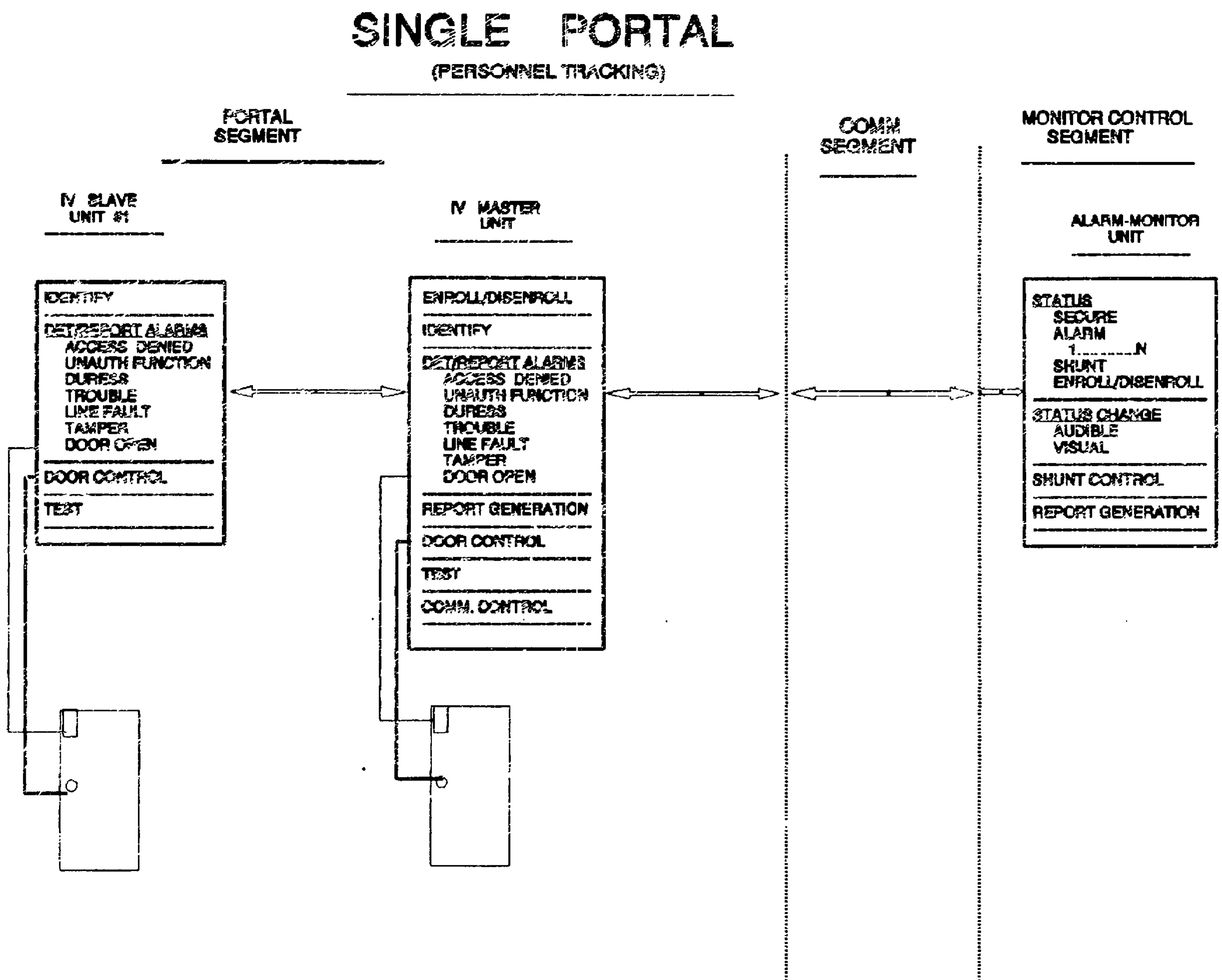
- Tamper (as a result of an attempt to remove the cover of the RCU).

(6) The RCU will have the capability to generate reports in pre-established format, or in specified format in response to a request by a system operator.

SINGLE PORTAL

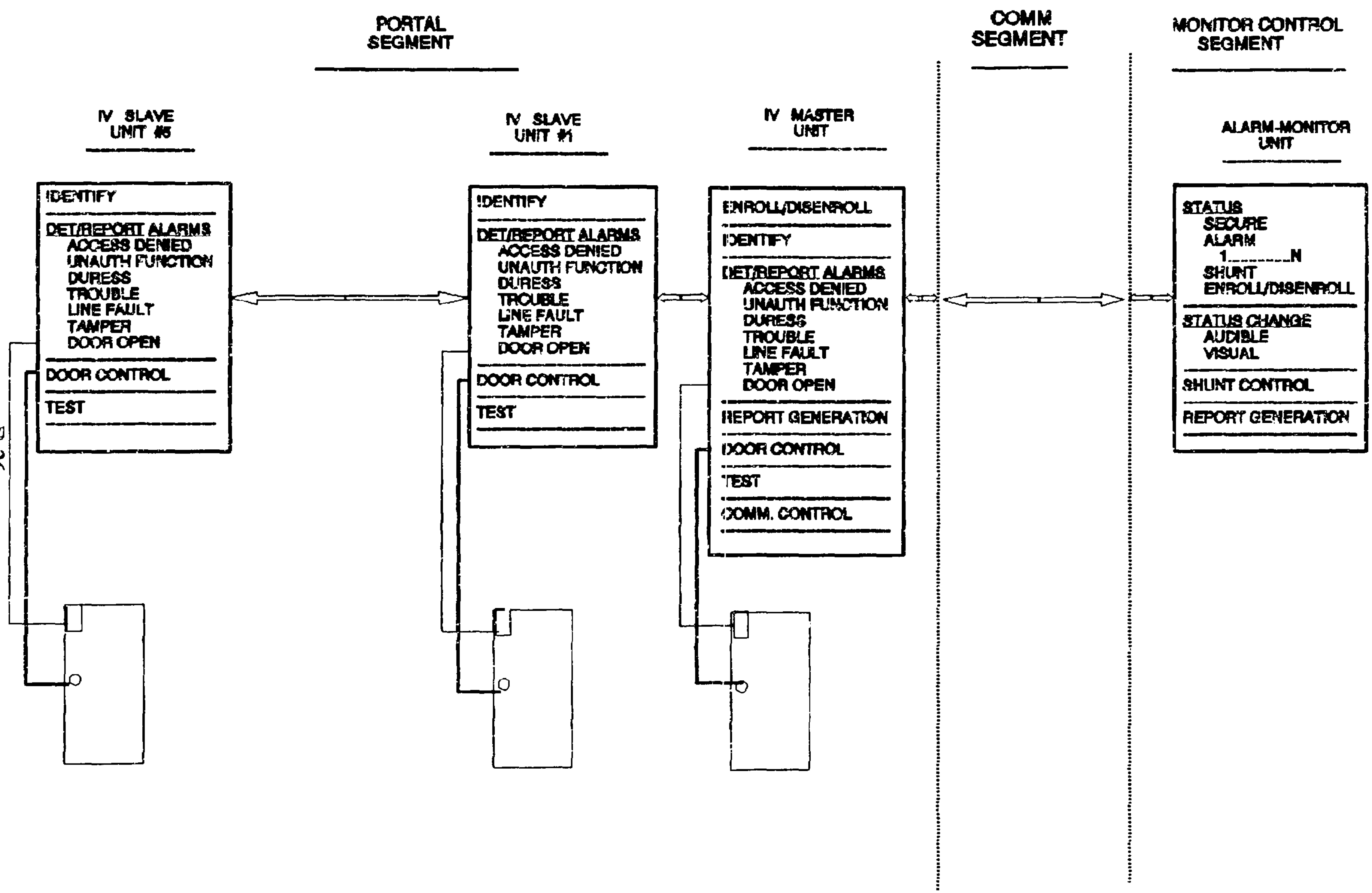


B-1. Single portal configuration.

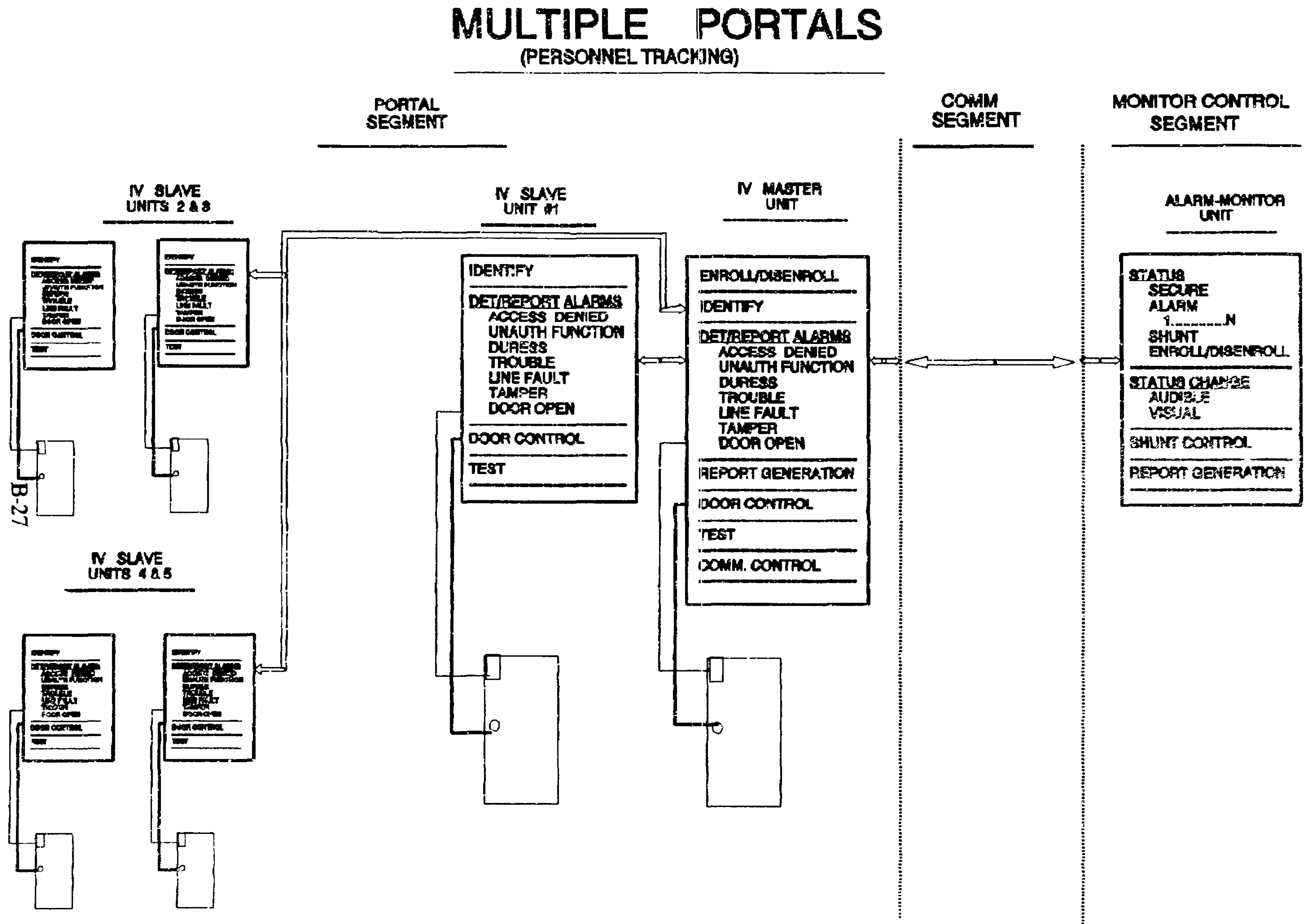


B-1. Single portal configuration (continued).

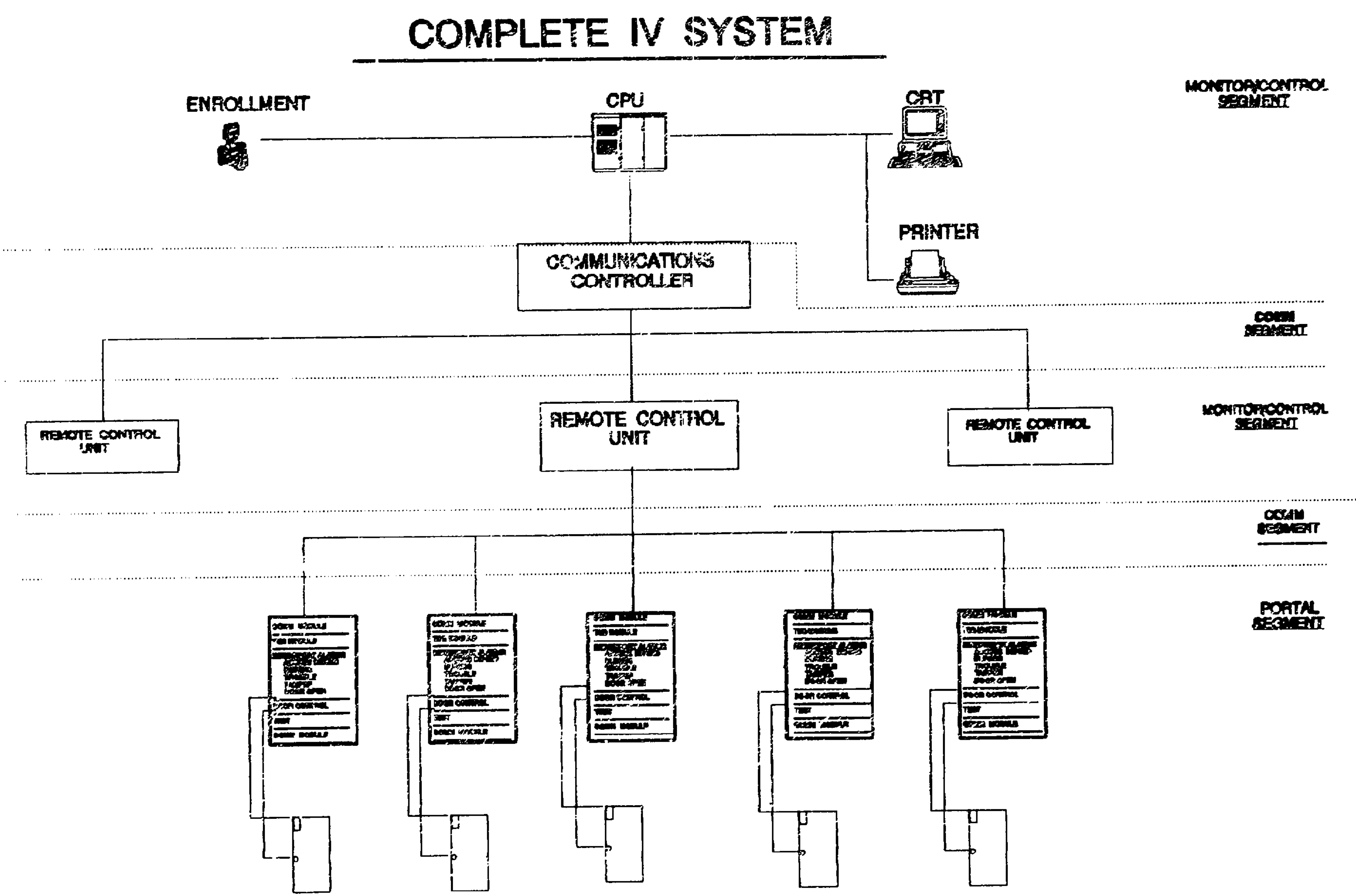
MULTIPLE PORTALS



B-2. Multiple portal configuration.



B-2. Multiple portal configuration (continued).



B-3. Complete IV system configuration.

APPENDIX C

TECHNICAL SYSTEM REQUIREMENTS

FOR A DOD IRIS RECOGNITION SYSTEM

C.1 INTRODUCTION.

C.1.1 Scope.

The purpose of this document is to specify the technical requirements for a DoD biometric identification system based on the use of the iris recognition technology. This document delineates the technical requirements for the initial "brassboard" system. The brassboard shall be suitable for further laboratory and field tests and evaluation in the course of development of the next level system. This document contains preliminary technical requirements for: design, interface, construction, and performance. This document will be used by IriScan Incorporated for the design, construction, and testing of the brassboard and to assess the brassboard for compliance with the stated requirements.

C.1.2 Purpose.

The purpose of the brassboard is to function as a biometric identification access control device using unique characteristics of the human iris as comparative parameters. The brassboard is to be a bench model version composed of hardware and software to implement the following general functions: video capture of the iris characteristics at a minimum range of 10 inches with a target range of 12 to 24 inches; analog and digital processing to convert, process, and analyze the video information; decision processing capability necessary to perform access verification in a timely manner; and communications to interface both with the individual using the IriScan and other access control support equipment.

The human-interface portion of the brassboard will be comprised of a monochrome charge-coupled device (CCD) camera and lens, mounted in/on a station suitable for video capture of the eye. The station will permit individuals of various heights to easily and quickly present themselves, have the video image of the iris captured and processed and receive verification of identification in sufficient time to permit throughput rates of twelve individuals per minute through a fully-configured access portal. The station will ultimately be configured so that the individual can activate the system without the use of hands, and adjust, if necessary, with only one hand.

The hardware and software that support the eye acquisition process will be composed of a 486/33 or 486/66 PC for digital processing and analysis, IriScan proprietary software, and communications circuitry to instruct the individual when to enter the portal. As an option, an input device (e.g. card reader, PIN keypad or pushbutton) may be provided to initiate the verification process if the system is to operate in a verification mode rather than the normal identification mode.

In its fully-configured form, the brassboard could act as a single-portal biometric access control device or as part of an overall access control system.

C.2 APPLICABLE DOCUMENTS.

The following documents of the issue shown form a part of this technical description document to the extent specified herein:

NOTE: The brassboard and subsequent production prototypes will be built to "best commercial standards" for high reliability performance. This equipment will not be required to meet military specifications. However, applicable specifications should be used as general design guidelines, when appropriate.

C.2.1 Government Documents.

MIL-STD-188-318	System and Subsystem Design and Engineering and Equipment Technical Standards for Closed Circuit Television (CCTV) Systems
MIL-STD-275	Printed Wiring for Electronic Equipment
MIL-STD-454	Standard General Requirements for Electronic Equipment
MIL-STD-781	Reliability Design Qualifications and Production Acceptance Tests, Exponential Distribution
MIL-STD-1472	Human Engineering Design Criteria for Military Equipment and Facilities
DIAM 50-3	Defense Intelligence Agency Manual 50-3, Physical Security Standards for Sensitive Compartmental Information Facilities

C.2.2 Non-Government Documents.

NFPA 70-1987	National Fire Protection Association (NFPA) National Electrical Codes (NEC)
UL 294	Underwriters' Laboratories (UL) Standard for Access Control System Units
UL 983	UL Standard for Surveillance Camera Units

RS-232-C	Electronic Industry Association (EIA) Interface Between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange.
RS-422-A	EIA Electrical Characteristics of Balanced Voltage Digital Interface Circuits.

C.2.3 Drawings.

DOD-MIL-T-31000

C.3 REQUIREMENTS.

This section provides the requirements for the brassboard in the following general areas: Item definition, system characteristics, component performance requirements and documentation.

C.3.1 Item Definition.

The brassboard is defined through a description of its functional subassemblies and interface requirements.

C.3.1.1 Functional Description. The brassboard performs the function of a biometric identification/verification device. The brassboard contains the hardware and software to acquire a video image of the unique characteristics contained in the iris, process and analyze this data, send a signal to an access-portal controller to permit or deny access into a restricted or controlled area and inform the user when access has been authorized or denied.

C.3.1.2 Image Acquisition Module Functions. The Image Acquisition Module (IAM) will house all necessary image acquisition components of the brassboard. The module will allow for positioning so that subjects (individuals) of various heights will be accommodated. Visual and/or audible feedback will be provided to aid in alignment and communication of instructions to the subject. Illumination for imaging will be provided. The module may include a secondary identification/activation device such as a card reader, numeric keypad, or pushbutton. All functions will be accomplished using only one hand.

a. Iris Image Acquisition. A high resolution CCD B&W video camera with a minimum focal point 12" from the panel will be utilized to capture an image of the subject's iris. Output from the video circuitry will be RS-170 analog video. The RS-170 signal will be sent to a video frame-grabber board for digitizing. The video frame-grabber will be an 8-bit device, as a minimum. The RS-170 signal may also feed a video LCD display or other form of display for feedback purposes. The digital information from the frame-grabber board will be directed to the image analysis processor. The verification decision will be provided to an external control unit for access control and/or to a device to inform the user of transaction results.

b. Communications. Communication to the image processor will be via two RS-232 serial ports and 1 parallel port with 8 Transistor to Transistor Logic (TTL) outputs and 4 TTL inputs.

C.3.1.3 Brassboard Computational Platform. The computational platform will be based on a dedicated 486 DX or SX microprocessor chip set. The platform will include:

486 DX or SX CPU,
1 M byte FLASH EPROM;
4 M byte RAM memory with capability for upgrade to 8 M bytes;
Serial and parallel communication ports;

Interface for an IDE hard disk drive (drive not included).
8 bit monochrome image digitizer;
Interface drivers (RS-232 and others) for data communications;
External I/O connectors; and
Enclosure and power supply.

a. Iris Signature Verification. The video information from the CCD camera will be processed and encoded into 2-D Gabor coefficients, resulting in an iriscode of 256 bytes as a minimum for each enrolled iris. The iriscode file will be compared to an iriscode resulting from a real-time captured image for verification.

b. Communication. The computational platform will communicate to an external access control unit via a 4-wire communications port utilizing Wiegand format. Communication with a host computer (if required) will be at 9600 baud in RS-422 format.

C.3.2 System Characteristics.

The brassboard shall perform as specified in the following paragraphs.

C.3.2.1 <u>Access Verification and Control Configurations</u>.

a. Stand-Alone. The system shall be able to function as a stand-alone device for identification or verification of an individual's identity for access authorization to a controlled facility or space. In the stand-alone mode, the system must provide for a minimum database of 4,000 enrollees.

b. Distributed System. When used in a multiple portal facility, the system shall provide for connection of portal-control readers to a central database for download of enrollee data and upload of events. The portal readers shall be capable of being interfaced to an existing card access system.

C.3.2.2 Enrollment System.

a. Process. The enrollment process shall be menu-driven and shall provide for input of administrative data relative to the enrollee. A means of flagging the enrollee's file for use by an external access control system shall be provided.

b. Time. The time required to successfully enroll a cooperative subject shall be no more than 120 seconds. This time shall not include the entry of administrative data.

c. Verification. The enrollment process shall include a verification that the system will identify the enrollee. The verification time shall be included in the enrollment time.

d. Number of Files. The system shall have the capability for enrollment of 40,000 individuals.

C.3.2.3 Portal Processing Requirements.

a. Processing Time. Portal control units shall be capable of verification and/or identification and rejection of an individual within 5 seconds of initiation of the identification/verification process. This time period shall include re-read times required due to false rejects.

b. Acceptance/Rejection. The Probability of False Acceptance (FA) shall be less than 0.1 % (0.001) and the Probability of False Rejection (FR) shall be less than 1 % (0.01) in any operating mode.

C.3.2.4 Communication.

a. Supervision. Communication lines between host and access control unit must be supervised. Both Class A and Class B line supervision, as defined in DIAM 50-3, will be incorporated into the communications system for any future production units.

b. Format. Data communicated between an access control system and the portal reader, if required, shall be in the industry-standard Wiegand format.

C.3.2.5 <u>Operating Environment</u>.

a. Temperature. The portal reader shall be capable of operation in temperatures within the range of 0 to 65 degrees Centigrade (32 to 150 degrees F).

b. Humidity. The portal reader shall be capable of operation in maximum 95 % relative humidity, non-condensing.

C.3.2.6 <u>Power</u>.

a. Voltage. 95 vac to 135 vac, 50 to 60 Hz, 150 VA max.

b. Backup. The portal reader shall be capable of operation for a minimum of 4 hours after loss of line power.

C.3.2.7 <u>Physical</u>.

a. Durability. The portal reader shall be housed in a rugged, tamper-proof cabinet. All cabinet doors or hatches shall be equipped with tamper switches.

b. Orientation. The portal reader shall be constructed to permit easy use by individuals, enable the acquisition of either eye, and the processing of the necessary data in sufficient time to permit 12 individuals per minute through the portal. The portal shall be suitable for one-hand operation.

c. Size and Weight. The biometric identification system shall not exceed 24" by 24" by 12", nor weigh more than thirty (30) pounds, as final production-unit goals.

d. Reliability. The system design will use concepts and commercially available components that will provide a high Mean Time Between Failures (MTBF). An MTBF of 10,000 hours is a desired goal for any production units. The design goal for Mean Time To Repair (MTTR) for production units is 1 hour or less.

C.3.2.8 Brassboard Interface Definitions. The brassboard is the interface between the individual requesting access and the monitoring system that controls access to a restricted space. In the case of a single portal, the brassboard will interface with a local portal-controller (electronic strike). In a multi-portal environment, the brassboard unit would interface not only with one or more local controllers, but must also interface with a system-wide monitoring computer (host). The brassboard also interfaces with the outside environment through its enclosures, cable terminations and ground planes. The brassboard interfaces with the individual attempting access through a portal and, when necessary, with a unit/system operator who enrolls personnel and performs other administrative system tasks.

a. System-Operator Interface.

(1) Functional. The system operator will communicate with the brassboard for the purpose of developing and manipulating system data; e.g., system status, enrollment parameters, etc. The interface will be controlled at the access-portal by the brassboard microprocessor in the stand-alone mode. In a multi-portal configuration, the system-operator communicates with the host computer.

(2) Physical. In the stand-alone mode, the system-operator will communicate to the brassboard through a communication port on the microprocessor, via an input device. In the multi-portal configuration, the system operator will communicate via a keyboard at the host computer.

b. Human Interface.

(1) Functional. An individual who wishes to gain access through the use of the brassboard will interface with the system through the Image Acquisition Module. The system will be capable of operating in either an identification or verification mode. If operating in the identification mode, the individual merely presents his eye to the system according to directions and training provided. If operating in the verification mode, the individual will either present an access control card and/or PIN or press a pushbutton to initiate the verification sequence. The system will prompt the individual on "proper orientation" and then display access denial or acceptance information.

(2) Physical. The human interface will permit individuals of varying heights to process though the portal.

c. Brassboard Computational Platform Interface.

(1) Functional. The brassboard unit will be mounted in an enclosed, environmentally-controlled space, within the protected portion of the facility.

(2) Physical. The brassboard system will be suitable for desk/table-top operation only for purposes of demonstrating feasibility of the technology.

d. Image Acquisition Module (IAM). The IAM for the brassboard unit will be designed for desk top mounting only for demonstration purposes. Production units of the system in the future will be suitable for a variety of mountings.

e. Power Interface.

(1) Functional. The brassboard system (Image Acquisition Module and Brassboard Computational Platform Module) will operate from 115 volts AC, 60 HZ, provided from facility power. Battery backup will be supplied for the IAM and the Brassboard Computational Platform Module in the event of power failure.

(2) Physical. The power will be supplied by flexible cable with separate conductors for phase, neutral and ground.

f. Image Acquisition Module Communication.

(1) Functional. The IAM will communicate to the microprocessor to provide video for processing and to receive data and control signals from the Computational Platform Module.

(2) Physical. A multi-conductor cable will connect the IAM to the Brassboard Computational Platform Module. No more than 50 feet will separate the two.

g. Brassboard Microprocessor Communication.

(1) Functional. In the stand-alone mode, the brassboard microprocessor will communicate to both a local access-control unit and a system-operator input device, through separate communication ports. In the multi-portal configuration, the brassboard microprocessor will communicate to both a local access-control unit and the system host, through separate communication ports.

(2) Physical. Two multi-conductor communication ports will be available for data transfer. The ports will include two RS-232 serial ports and 1 parallel port with 8 TTL outputs and 4 TTL inputs.

C.3.3 Component Performance Requirements.

The brassboard and its subassemblies will perform as specified in the following sections.

C.3.3.1 Brassboard Computational Platform. The brassboard computational platform will consist of market-available board-level components that will be selected during the development process. The components will be selected as a "best fit" between performance and cost and will meet, as a minimum, the following requirements:

a. A 486 32-bit microprocessor, running at a minimum clock speed of 33 MHz; minimum of 28 MIPS (million instructions per second), 60-80 NS instruction cycle.

b. At least 1 Mbyte of FLASH EPROM

c. 4 Mbyte DRAM with provision for upgrade to 8 Mbyte

d. A minimum of 2 RS-232 serial communication ports

e. 1 parallel communication port with 8 TTL outputs and 4 TTL inputs

f. Interface for an IDE hard disk drive

g. A 640 X 480 X 8 bit monochrome image digitizer

h. External I/O connectors

i. Off-the-shelf plastic enclosure and A/C power supply

C.3.3.2 Image Acquisition Module (IAM). The IAM will consist of market-available board-level components that will be selected during the development process. The components will be selected as a "best fit" between performance and cost and will meet as a minimum the following requirements:

a. A monochrome CCD video camera with a minimum resolution of 754 pixels (H) by 488 pixels (V). The device will have a minimum face-plate illumination of 0.05 fc.

b. A liquid crystal display (LCD), video tube display, mirror, or other form of image display to facilitate alignment of the eye and communication with subject.

c. An illumination source.

d. An optical lens system.

C.3.3.3 <u>Central Host Computer (NOT PROVIDED)</u>. The central host computer in a typical commercial security system is a standard product-line unit manufactured by IBM or an IBM clone. The brassboard will be able to interface with a host computer which meets the following requirements:

a. A 32-bit microprocessor running at 66 MHz;

b. 4 Mbytes of non-volatile memory;

c. 8 Mbytes of random-access memory;

d. A 1.44 MB floppy drive;

e. An IDE 210 MB hard drive;

f. A VLB IDE HD/FD and I/O controller;

g. A VLB 32 bit SVGA 1 MB card (1280 x 1024 Res);

h. An SVGA monitor w/ .28 dp NI; and

i. A laser printer.

C.3.4 Documentation.

C.3.4.1 Technical Manual. The brassboard will be delivered with a set of instructions describing initial set-up procedures and software and system operation. The documentation will contain commercial manuals for all commercial system components and information on any IriScan-developed boards or subassemblies.

C.3.4.2 Drawings. The brassboard will be supplied with developmental drawings for all assemblies, in accordance with DOD-MIL-T-31000 requirements.

C.3.4.3 Brassboard Design Manual. A manual which includes a description of the brassboard and any design calculations and assumptions will be supplied.

C.3.4.4 Software Description Document. Since the software used in the iris recognition system is identified as RESTRICTED software having been developed totally at our own expense, only a description of the software will be provided for retention by the government, not any software itself.

APPENDIX D

OPERATIONAL SCENARIOS

DOD IRIS RECOGNITION SYSTEM

D.1 ENROLLMENT.

D.1.1 General.

The enrollment process will vary depending on the configuration of the system. For example, in a single portal system, the enrollment function can (but not necessarily must) occur at the portal. The administrative determination that a person has the right and need for entry/access to the area can be made elsewhere for convenience, but if there is only one identifier/verifier (IV), the enrollment must occur at its location.

The system will be designed for easy utilization by cooperating enrollees; but, if difficulties are encountered, the following guidance steps will be followed.

D.1.2 Positioning.

An enrollee will be positioned on some clearly marked spot as an initial, crude form of alignment. Where practical, the enrollee can sit in a chair to enhance stability. The practicality of this portion of the scenario is a determination for the system operator. It may be practical at the portal, if volume is low.

D.1.3 Alignment.

The operator will instruct the enrollee to position his head such that the iris of the right eye is centered on a marker in the lens of the IV.

D.1.4 Focus.

The operator will instruct the enrollee to move forward or backward slightly until the iris is in focus.

D.1.5 Activation.

The operator will activate the live-enroll function of the IV and instruct the enrollee to remain motionless until the IV has acquired and encoded six frames of the iris. An audible signal will alert the operator and enrollee when this has been completed. The system averages the Hamming Distances of the iriscodes and enters the iriscode with the Hamming Distance closest to that average into the database. The operator accepts the enrollment by key stroke if the Hamming Distance is below the criteria established by the operator. (Such criteria, set now at .32 for the early laboratory device, should be determined by the security staff and codified by policy.)

D.1.6 Second Eye.

The procedures above will be repeated for the left eye.

D.1.7 Validation.

The system operator will place the IV in the live-recognition mode and verify the capability to identify each of the enrollee's irises.

D.1.8 Administrative Data.

The operator will key in a tag-code for linking of the iriscode to necessary administrative data (name, SS#, etc.).

D.2 ENTRY/EXIT -- NORMAL.

D.2.1 Identification Mode.

a. The entrant will position himself in front of the IV and accomplish the actions described in paragraphs 1.2, 1.3, and 1.4, above, relative to positioning, alignment, and focus

b. The IV will construct the iriscode and compare it to the database files for a match. If there is not a match, the system will not operate the strike, will initiate an "Access Denied: Unidentified Person" alarm at the Monitor/Control segment, will activate the Access Denied Light at the portal, and will store the iriscode of the denied entrant in a separate, retrievable file.

c. If there is a match, the system will determine if the entrant is authorized to enter that area at the current time and day of the week. If the would-be entrant is not authorized to be in the area, the system will not operate the strike, will initiate an "Access Denied: Unauthorized Time/Unauthorized Portal" alarm (as appropriate), will activate the Access Denied Light at the portal, and will store the iriscode of the denied entrant in a separate, retrievable file. If the entrant is authorized, the system will activate the strike. Under most circumstances the sound of the strike activating will provide sufficient audible indication.

d. The entrant will proceed through the portal promptly and secure it behind him, ensuring that no one tailgates.

e. The system will monitor the door-open indication, and initiate an alarm if the portal remains open beyond a preset period.

D.2.2 Verification Mode.

a. The entrant will activate the IV by card or PIN upon arrival at the portal.

b. The entrant will position himself in front of the IV and accomplish the actions described in paragraphs 1.2, 1.3, and 1.4, above, relative to positioning, alignment, and focus.

c. The IV will construct the iriscode from the entrant and compare it to the iriscode encoded on the card, or in the database, for a match. If there is not a match, the system will not operate the strike, will activate the Access Denied Light at the portal, and will initiate an "Access Denied: Unidentified Person" alarm at the Monitor / Control segment.

d. If there is a match, the system will determine if the entrant is authorized to enter that area at the current time and day of the week. If the would-be entrant is not authorized to be in the area, the system will not operate the strike, will initiate an "Access Denied: Unauthorized Time / Unauthorized Portal" alarm (as appropriate), will activate the Access Denied Light at the portal, and will store the iriscode of the denied entrant in a separate, retrievable file. If the entrant is authorized, the system will activate the strike. Under most circumstances the sound of the strike activating will provide sufficient audible indication.

e. The entrant will proceed through the portal promptly and secure it behind him, ensuring that no one else tailgates.

f. The system will monitor the door-open indication, and initiate an alarm if the portal remains open beyond a preset period.

D.2.3 Exit.

If Personnel-Tracking is not a requirement, the interior of the portal can be equipped with a pushbutton that activates the strike from the inside, while shunting the alarm. The interior of the portal must also be equipped with manual panic-hardware to enable rapid exit of personnel, notwithstanding the power status of the facility. The system will be configured to initiate a "Portal Open: Emergency Exit" alarm when that means of egress is used.

D.3 ENTRY / ACCESS TRACKING MODE.

D.3.1 General.

While the configuration of the portal will change with the addition of a second IV inside the space, the entry procedures outlined in the scenarios above will remain the same.

D.3.2 Entrant Requirements.

Personnel granted access to the protected space will require indoctrination to insure that they utilize the IV each time they exit the area.

D.3.3 System Requirements.

Notwithstanding Personnel-Tracking rules and procedures established by the security staff, the interior of the portal must also be equipped with manual panic-hardware to enable rapid exit of personnel, regardless of the power status of the facility. The system will be configured to initiate a "Portal Open: Emergency Exit" alarm when that means of egress is used.

D.3.4 Re-Entry.

Absent some system-operator initiated action to override, the Personnel-Tracking option of the system would recognize that no exit-transaction for that individual occurred since the previous entrance-transaction and would result in no strike activation, energizing of the Access Denied Light at the portal, and initiation of an "Access Denied: No Exit" alarm.

APPENDIX E

ESTIMATE OF COSTS TO COMPLETE DEVELOPMENT

DOD IRIS RECOGNITION SYSTEM

OPTION 1
PHASE II
DNA001-93-C-0137
DECEMBER 17, 1993

ADDITIONAL ENGINEERING DEVELOPMENT COSTS FOR BRASSBOARD UNIT
DEVELOPMENT OF IDENTIFICATION/VERIFICATION (IV) TECHNOLOGY/METHODOLOGY
DEFENSE NUCLEAR AGENCY
JANUARY 1, 1994 THROUGH DECEMBER 31, 1994

COST BREAKDOWN

SALARIES W/FRINGE BENFTS	TRAVEL & PER DIEM	MATERIALS & OTHER	COMBINED INDIRECT COST	ESTIMATED COST	COM	FIXED FEE	TOTAL
$145,501	$3,800	$15,360	$112,971	$277,632	$0	$23,599	$301,231

OPTION 1
PHASE II
DNA001-93-C-0137
DECEMBER 17, 1993

WORK BREAKDOWN STRUCTURE - SKILLS AND LEVEL OF EFFORT

IRISCAN TASK NUMBER OPTION 1	CUSTOMER REF TASK SOW	DESCRIPTION PHASE II BRASSBOARD IV SYSTEM	SR ANALYST/ PROG MNGR	SENIOR ANALYST	ANALYST	SENIOR ENGINEER	ENGINEER	SENIOR SCIENTIST MATHEMATICIAN	SENIOR SCIENTIST	SENIOR SCIENTIST	ADMIN/ SECRETARY	IRISCAN TOTAL
	3 2											
I	3 2 1	PROTOTYPE DEVELOPMENT										
1-100		DEFINE SYSTEM ARCHITECT	24	24	32	56	72	8	2	2	16	236
1-200		DEFINE DETAILED INTERFACES	24	24	32	56	180	8	2	2	16	344
1-300		DEVELOP HW & SW SPECIFICATIONS	24	24	32	56	72	8	2	2	32	252
1-400		DEVELOP PROTOTYPE										
1-410		BRASSBOARD HARDWARE										
1-411		TRANSITION LABORATORY MODEL	8	16	16	56	80	2	2	2	0	182
1-412		PREPARE SYSTEM DESIGN	8	16	16	56	120	8	2	2	8	236
1-413		ASSEMBLE & EVALUATE PROTOTYPE	8	16	15	56	80	8	2	2	0	188
1-414		MODIFY TO MEET OPNL PERF REQUIREMENT	12	16	16	56	80	8	2	2	0	192
1-420		SOFTWARE										0
1-421	3 1 1	MODIFY IRISCAN PROPRIETARY SOFTWARE	14	8	8	32	40	8	2	2	0	114
1-422		MODIFY SUPPORT SYS SOFTWARE	14	8	8	32	48	20	2	2	0	134
1-423		CODE TECHNICAL SYSTEM SOFTWARE	8	8	8	32	8	30	2	2	0	98
1-500		DOCUMENT WITH DOD-MIL-T-31000 DRAWINGS	8	8	8	24	120	8	2	2	0	180
1-600		UPDATE COST ESTIMATE FOR DEPLOYABLE SYS	14	8	8	24	40	8	2	2	6	112
II	3 2 2	TEST PLAN										
II-100		DEFINE TEST OBJECTIVES	16	4	8	16	40	4	2	2	8	100
II-200		DEVELOP EVALUATION CRITERIA	16	4	8	16	40	4	2	2	8	100
II-300		IDENTIFY TEST BED	16	4	8	16	16	4	2	2	0	68
II-400		DEVELOP TEST POA&M	15	4	16	16	16	4	2	2	8	84
II-500		PUBLISH TEST PLAN	8	4	16	16	16	4	2	2	16	84
III	3 2 3	PROTOTYPE TEST & PROOF OF CONCEPT										
III-100		CONDUCT TEST	32	6	48	16	72	0	0	0	0	174
III-200		EVALUATE/ANALYZE RESULTS	16	6	32	16	40	16	0	0	0	126
III-300		DOCUMENT RESULTS IN FINAL REPORT	16	6	32	16	24	8	0	0	24	126
III-400		DEMONSTRATE PROOF OF CONCEPT	16	6	8	16	24	0	0	0	0	70
IV	CDRL	REPORTING REQUIREMENTS										
IV-100		MONTHLY LETTER PROGRESS REPORT	40	2	0	0	0	0	0	0	18	60
IV-200		QUARTERLY COST PERFORMANCE REPORT	16	2	0	0	0	0	0	0	18	36
IV-300		PHASE II DRAFT FINAL REPORT	48	8	40	16	48	24	2	2	32	220
IV-400		PHASE II CAMERA READY FINAL REPORT	16	8	16	8	32	8	2	2	32	124
		TOTAL HOURS	438	240	432	704	1308	200	38	38	242	3640

APPENDIX F

ESTIMATE OF CORE SYSTEM COSTS

DOD IRIS RECOGNITION SYSTEM

ESTIMATED
DoD IRIS RECOGNITION SYSTEM
CORE SYSTEM COSTS
(PER- PORTAL)

IRIS IDENTIFICATION VERIFICATION SYSTEM

		ESTIMATED COST
1. COMPUTATIONAL PLATFORM		
a. x86 microprocessor chip set		$500
b. 8-bit monochrome A to D image digitizer		200
c. 8 M byte RAM memory		350
d. 2 M byte FLASH EPROM		85
e. Miscellaneous hardware components		150
f. Communication drivers		75
g. Power supply		40
h. Enclosure		80
	Sub-total	$1,480
2. IMAGE ACQUISITION MODULE		
a. 1/3 " format monochrome CCD video chip		$250
b. Optical lens unit		400
c. Liquid crystal display or video tube display		400
d. Beam splitter		30
e. Luminaire		75
f. Power supply		40
g. Enclosure		40
h. Miscellaneous hardware/components		80
	Sub-total	$1,315
3. SOFTWARE LICENSE FEE (Paid to IriScan, Inc.)		
Cost per Portal/unit		$800
4. CENTRAL HOST COMPUTER ALLOCATION ***		$240
(Allocation based on total of 10 portals)		
	TOTAL PER- PORTAL ESTIMATE	$3,835.00

CENTRAL HOST COMPUTER (OPTIONAL) $1,500

COMPUTER
- 32 bit microprocessor, x86/ 66 MHz
- 4 M byte non-volatile memory
- 1.44 M byte floppy drive
- IDE 340 M byte hard drive
- 15 " SVGA color monitor
- AT I/O card
- Verticle case and power supply
- 101 key enhanced keyboard
- DOS 6.2

PRINTER (ONE OF SEVERAL AVAILABLE LASER PRINTERS)	$600
SOFTWARE LICENSE (TYPICAL DISTRIBUTED SYSTEM FOR ENTRY/ACCESS CONTROL)	$300
TOTAL	$2,400

***
NOTE: The CENTRAL HOST COMPUTER is considered optional since the SOW required an estimate of the portal IV unit only. The Central Host Computer would be used when the system configuration required that the portal units be integrated with a central monitoring unit. If a Central Computer is required, the estimated cost would be prorated over the total number of portal units

APPENDIX G

ESTIMATE OF SYSTEM INSTALLATION COSTS

DOD IRIS RECOGNITION SYSTEM

The installation costs for the DoD IriScan system are directly dependent upon a number of variables, to include type of installation required, system configuration, location, facility construction, environmental conditions, availability of utilities, etc. Until such time as detailed site surveys are performed at the location programmed to receive the system, it must be recognized that any cost estimate is to be considered a gross estimate only. At this stage in the development cycle, sufficient information is not available to allow other than a gross estimate. However, based on installation costs for similar electronic products used for entry/access control, it is estimated that per-portal installation costs for a DoD IriScan unit would average $500. This estimate assumes minimal demolition/construction costs to install the unit in an interior, wall-mounted configuration.

APPENDIX H

SYSTEM DESIGN CONCEPT

DOD IRIS RECOGNITION SYSTEM

H.1 INTRODUCTION.

The design of the DoD Iris Recognition System will make maximum utilization of commercially-available, off-the-shelf components. Standardized, industry-proven and accepted materials and parts will be used to the maximum extent possible, within the constraints of cost and performance. To the extent possible, the design, selection, and integration of materials and parts will adhere to the following concepts.

H.2 COMPONENTS.

System components should:

a. Utilize solid-state technology throughout the design.

b. Be interchangeable with any other like component.

c. Reflect technology that has an established future growth pattern, e.g., the Intel family of X86 microprocessor chip sets.

d. Utilize elements with low power requirements.

e. Be mounted on printed circuit boards meeting UL standards.

f. Include high maintainability and integration capabilities.

H.3 MODULARITY.

The system should be capable of increasing performance based on addition of modular components or a selection of software modules. To the extent possible, increased performance should be accomplished through software selection of options rather than the addition of hardware.

H.4 INTERCHANGEABILITY.

The system should be constructed with off-the-shelf Lowest Replaceable Unit (LRU) assemblies and components that are physically, functionally and electrically interchangeable. Custom-designed, unique, or unusual items should not be used. Maintenance should be performed by replacement of LRU modules.

H.5 HUMAN INTERFACE.

The system design should reflect industry-accepted human engineering practices. Human factors engineering principles should be used to ensure the effectiveness of the man-machine interface and to enable use and maintenance of the system with minimal training.

APPENDIX I

STRAWMAN DEPLOYMENT POA&M

DOD IRIS RECOGNITION SYSTEM

Schedule Name : DNA STRAWMAN DEPLOYMENT POA&M
Responsible :
As-of Date : 22-Nov-93 8:00a Schedule File : STRWPOAM

```
 94                      95                        96                      97                       98                      99
 Jan AprJun SepNovJanMar JunAugOct Jan AprJunAug Nov FebApr JulSepNov Feb MayJul Oct Jan AprJunAugOct
 3   1  1   1  1  2  1   1  1  2   2   1  3  1   1   3  1   1  2  3   2   1  1   1   4   1  1  2  1
```

Task Name	Start Date	Duration	End Date
START	31-Jan-94	0.0	31-Jan-94
BRASSBOARD DEVELOPMENT	31-Jan-94	10.0 m	2-Dec-94
TRANSITION TO 6.4	5-Dec-94	1.0 m	3-Jan-95
FULL-SCALE ENG DEV.	4-Jan-95	15.0 m	23-Apr-96
PROCUREMENT(3080)	24-Apr-96	24.0 m	1-Jun-98
DEPLOYMENT	30-Sep-9_	34.0 m	22-Sep-99

Detail Task — Summary Task — ***** Baseline
(Progress) — (Progress) — Conflict
(Slack) — (Slack) — Resource delay
Progress shows Percent Achieved on Actual — o Milestone

Scale: 3 weeks per character

TIME LINE Gantt Chart Report, Strip 1

APPENDIX J

LIST OF ABBREVIATIONS AND ACRONYMS

Acquired Immune Deficiency Syndrome	AIDS
Advanced Entry Control System	AECS
alternating current	AC
American Society for Industrial Security	ASIS
Army Research Laboratory	ARL
IBM 80286 CPU	AT
automated teller machine	ATM
black and white	B&W
cathode ray tube	CRT
centigrade	c
Central Intelligence Agency	CIA
central processing unit	CPU
charged coupled device	CCD
closed circuit television	CCTV
Commerce Business Daily	CBD
communications	comm
compact disk	CD
Computational Platform	CP
cost of money	COM
Crossover Error Rate	CER
Defense Nuclear Agency	DNA
Defense Technical Information Center	DTIC
Defense Intelligence Agency Manual	DIAM
Department of Defense	DoD
detect	det
dispersion	dp
Electronic Industry Association	EIA
electronically programable read-only memory	EPROM
False Acceptance	FA
False Rejection	FR
Fahrenheit	F
Full-Scale Engineering Development	FSED
floppy disk	FD
footcandle	fc
hard disk	HD
hardware	HW
hertz	Hz
high speed EPROM	FLASH
identification	ID
integrated drive electronics	IDE
identification verification	IV
Image Acquisition Module	IAM
Immigration & Naturalization Service	INS
Information Systems Network	ISN
input/output	I/O
intrusion detection system	IDS
IV Master Unit	IMU
IV Slave Unit	ISU
liquid crystal display	LCD
local area network	LAN
Los Alamos National Laboratory	LANL
Lowest Replaceable Unit	LRU
magnetic stripe card	MSC

Massachusetts Institute of Technology	MIT	Plan of Action & Milestones	POA&M
Mean Time Between Failures	MTBF	production	prod
Mean Time To Repair	MTTR	random access memory	RAM
megabyte	Mbyte, MB	Remote Control Unit	RCU
megahertz	MHz	Research & Development	R&D
military specification	MILSPEC	research, development, test & evaluation	RDT&E
military standard	MILSTD	resolution	Res
million instructions per second	MIPS	Sandia National Laboratories	SNL
nano-second	NS	software	SW
National Electrical Codes	NEC	Statement of Work	SOW
National Fire Protection Association	NFPA	Support System Software	SSS
National Security Agency	NSA	Super VGA video graphics array	SVGA
National Technical Information Service	NTIS	system	SYS
non-interlaced	NI	Technical System Functions	TSF
operational	OPNL	Technical System Software	TSS
Operational Performance Requirements	OPR	temperature	temp
Operational Requirements Document	ORD	The Analytical Sciences Corporation	TASC
performance	PERF	transistor-to-transistor logic	TTL
personal identity verifier	PIV	2-dimensional	2-D
Personal Identification Number	PIN	Underwriters' Laboratories	UL
		uninterrupted power supply	UPS
		video local bus	VLB
		voltage alternating current	vac

DISTRIBUTION LIST

DNA-TR-94-6

DEPARTMENT OF DEFENSE

ADVANCED RESEARCH PROJECT AGENCY
ATTN: EAO
ATTN: STO N DOHERTY

DEFENSE INTELLIGENCE AGENCY
ATTN: DIW-4

DEFENSE NUCLEAR AGENCY
2 CY ATTN: IMTS
3 CY ATTN: NOSA
ATTN: OPNA
ATTN: OPNO

DEFENSE TECHNICAL INFORMATION CENTER
2 CY ATTN: DTIC/OC

OASD
ATTN: DASD CI & SCM

OFFICE OF THE SECRETARY OF DEFENSE
ATTN: DNA OATSD AE LIASON OFFICE

U S CENTRAL COMMAND
ATTN: CCJ3
ATTN: CCPM

U S EUROPEAN COMMAND/ECJ2-T
ATTN: ECJ5N

UNDER SECRETARY OF DEFENSE (ACQ)
ATTN: ODDR&E/TS/LS

DEPARTMENT OF THE ARMY

ARMY RESEARCH INSTITUTE
ATTN: COMMANDER

DEPUTY CHIEF OF STAFF FOR PERSONNEL
2 CY ATTN: DAMO-ODL

OFFICE OF THE CHIEF OF ENGINEER
ATTN: CEMP-ET

U S ARMY BELVOIR RD&E CTR
ATTN: AMSAT-I-WTP
ATTN: SATBE-JIS
ATTN: STRBE-ES
ATTN: STRBE-N
ATTN: STRBE-X
ATTN: STRBE-ZTS DR STEINBACH

U S ARMY ELECTRONIC WARFARE LAB
ATTN: DELEW-I-S

U S ARMY LABORATORY COMMAND
ATTN: DR D HODGE
ATTN: SLCHE-CC-LHD HARRAH
ATTN: SLCHE-CS

U S ARMY MILITARY POLICE SCHOOL
ATTN: ATZN-MP-CD
ATTN: ATZN-MP-DE
ATTN: ATZN-MP-TB
ATTN: ATZN-MP-TS

U S ARMY NUCLEAR & CHEMICAL AGENCY
ATTN: MONA-SU

U S ARMY TRAINING AND DOCTRINE COMD
ATTN: ATCD-N

USA 1ST SOCOM (ABN)
ATTN: ASOF-OGO-N4

USAS4A
ATTN: AMXSY-CA

DEPARTMENT OF THE NAVY

DAVID TAYLOR RESEARCH CENTER
ATTN: CODE 1203

SPACE & NAVAL WARFARE SYSTEMS CMD
ATTN: PME-121-3

STRATEGY AND POLICY DIVISION
ATTN: NO9N
ATTN: OPNAV 981N

U.S. ATLANTIC COMMAND
ATTN: J324

US MARINE CORPS
ATTN: POS-20
ATTN: POS-30

DEPARTMENT OF THE AIR FORCE

AERONAUTICAL SYSTEMS C NTER
ATTN: SP

AIR COMBAT COMMAND/SPSC
ATTN: ACC/SP

AIR FORCE MATERIEL COMMAND
ATTN: AFMC/SP

DEPARTMENT OF THE AIR FORCE
ATTN: AF/RDST

MILITARY AIRLIFT COMMAND AMC/SP
ATTN: SP

PACAF/LGWSN
ATTN: SP

TECHNICAL DIRECTOR (NWI)
ATTN: NTSMS

U S AIR FORCE IN EUROPE/SP
ATTN: ATTN USAFE/SPO
ATTN: USAFE/SPP

USAF/SP
ATTN: USAF/SPO
ATTN: USAF/SPP

DEPARTMENT OF ENERGY

ASSOCIATED UNIVERSITIES, INC
ATTN: DOCUMENT CUSTODIAN

DEPARTMENT OF ENERGY
ATTN: DASMA DP-20

SANDIA NATIONAL LABORATORIES
ATTN: DIV 9538
ATTN: ORG 9503 J W KANE
5 CY ATTN: ORG 9549

OTHER GOVERNMENT

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
ATTN: L ELAISON

U S SECRET SERVICE
ATTN: LIBRARY

DEPARTMENT OF DEFENSE CONTRACTORS

IRISCAN, INC
2 CY ATTN: C B KUHLA
2 CY ATTN: D R RICHARDS
2 CY ATTN: G O WILLIAMS
2 CY ATTN: J E SIEDLARZ
2 CY ATTN: J T MCHUGH

JAYCOR
ATTN: CYRUS P KNOWLES

KAMAN SCIENCES CORP
ATTN: DASIAC

KAMAN SCIENCES CORPORATION
ATTN: DASIAC